

SOLUCIÓN DE DOS ESTUDIOS DE CASO BAJO EL USO DE TECNOLOGÍA  
CISCO

ALEJANDRO YEPES JARAMILLO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA –UNAD  
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI  
INGENIERÍA DE SISTEMAS  
FACATATIVA  
2021

SOLUCIÓN DE DOS ESTUDIOS DE CASO BAJO EL USO DE TECNOLOGÍA  
CISCO

ALEJANDRO YEPES JARAMILLO

Diplomado de opción de grado presentado para optar el título de INGENIERÍA DE  
SISTEMAS

DIRECTOR:  
JAVIER RICARDO VASQUEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA –UNAD  
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI  
INGENIERÍA DE SISTEMAS  
FACATATIVA  
2021

Nota de Aceptación

---

---

---

---

Presidente del Jurado

---

Jurado

---

Jurado

FACATATIVA, 28 de noviembre de 2021

## CONTENIDO

CONTENIDO .....	4
LISTA DE TABLAS .....	5
LISTA DE FIGURAS .....	6
GLOSARIO .....	8
RESUMEN .....	9
ABSTRACT .....	10
INTRODUCCIÓN .....	11
DESARROLLO .....	12
1.  ESCENARIO 1 .....	12
2.  ESCENARIO 2 .....	23
CONCLUSIONES .....	71
BIBLIOGRAFÍA .....	72

## LISTA DE TABLAS

Tabla 2. Tabla de direccionamiento LAN1. ....	13
Tabla 4. Tabla de direccionamiento LAN2. ....	14
Tabla 1. Tabla de direccionamiento para el primer escenario. ....	14
Tabla 7. Lista de configuraciones para aplicar en R1. ....	14
Tabla 8. Tabla de configuraciones en S1. ....	16
Tabla 9. Configuración de direccionamiento en PC-A. ....	18
Tabla 10. Configuración de direccionamiento en PC-B. ....	19
Tabla 11. Tabla de configuraciones para inicializar y volver a cargar los routers y los switches. ....	24
Tabla 12. Configuración de la computadora de Internet. ....	26
Tabla 13. Configuración de R1. ....	27
Tabla 14. Configuración de R2. ....	29
Tabla 15. Configuración de R3. ....	32
Tabla 16. Configuración de S1. ....	35
Tabla 17. Configuración de S3. ....	36
Tabla 18. Verificación de la conectividad de la red. ....	38
Tabla 19. Tabla de configuración de seguridad, VLAN y routing entre VLAN en S1. ....	40
Tabla 20. Tabla de configuración de seguridad, VLAN y routing entre VLAN en S3. ....	42
Tabla 21. Tabla de configuración de subinterfaces en R1. ....	44
Tabla 22. Tabla de verificaciones de la conectividad de la red. ....	46
Tabla 23. Tareas de configuración para R1. ....	49
Tabla 24. Tabla de configuración para R2. ....	50
Tabla 25. Tareas de configuración para R2. ....	51
Tabla 26. Verificación de la información de OSPF. ....	52
Tabla 27. Tabla de configuración DHCP en R1 para las VLANs 21 y 23. ....	57
Tabla 28. Lista de tareas de configuración NAT estática y dinámica en R2. ....	59
Tabla 29. Tabla de verificación del protocolo DHCP y la NAT estática. ....	60
Tabla 30. Lista de tareas de configuración NTP. ....	63
Tabla 31. Lista de tareas de configuración y verificación de listas de control de acceso en R2. ....	64
Tabla 32. Lista de tareas de verificación de comando CLI. ....	67

## LISTA DE FIGURAS

Figura 1. Topología propuesta para el escenario 1.....	12
Figura 2. Presentación de la topología en packet tracer.....	13
Figura 3. Configuraciones de red del host con el comando ipconfig /all en PC-A..	19
Figura 4. Evidencia de la configuración del PC-B. ....	20
Figura 5. Prueba de conectividad entre PC-A y SVI del switch S1. ....	21
Figura 5. Prueba de conectividad entre PC-A y las interfaces de R1. ....	21
Figura 5. Prueba de conectividad entre PC-A y PC-B. ....	22
Figura 6. Topología propuesta para el escenario 2.....	23
Figura 6. Verificación de que la base de datos de VLAN no esté en la memoria flash en S1.....	25
Figura 6. Verificación de que la base de datos de VLAN no esté en la memoria flash en S2.....	26
Figura 7. Configuración del Servidor de Internet.....	27
Figura 8. Validación de ping desde R1 a R2.....	39
Figura 9. Validación de ping desde R2 a R3.....	39
Figura 10. Validación de ping desde Servidor de Internet a su Gateway.....	40
Figura 11. Validación de ping desde S1 a R1, dirección VLAN 99. ....	47
Figura 12. Validación de ping desde S3 a R1, dirección VLAN 99. ....	47
Figura 13. Validación de ping desde S1 a R1, dirección VLAN 21. ....	48
Figura 14. Validación de ping desde S3 a R1, dirección VLAN 23. ....	48
Figura 15. Verificación del ID del proceso OSPF, del router, las redes de routing y las interfaces pasivas en R1.....	53
Figura 16. Verificación de las rutas OSPF en R1.....	53
Figura 17. Verificación de sección de OSPF de la configuración en ejecución en R1.....	54
Figura 18. Verificación del ID del proceso OSPF, del router, las redes de routing y las interfaces pasivas en R2.....	54
Figura 19. Verificación de las rutas OSPF en R2.....	55
Figura 20. Verificación de sección de OSPF de la configuración en ejecución en R2.....	55
Figura 21. Verificación del ID del proceso OSPF, del router, las redes de routing y las interfaces pasivas en R3.....	56
Figura 22. Verificación de las rutas OSPF en R3.....	56
Figura 23. Verificación de sección de OSPF de la configuración en ejecución en R3.....	57
Figura 24. Verificación del direccionamiento DHCP en PC-A.....	61
Figura 25. Verificación del direccionamiento DHCP en PC-C.....	62
Figura 26. Verificación del ping entre PC-A y PC-C.....	62
Figura 27. Verificación de la conexión al servidor web desde el PC-A. ....	63
Figura 28. Verificación de la configuración NTP en R1.....	64
Figura 29. Verificación de la ACL en PC-A.....	66
Figura 30. Verificación de la ACL en R1.....	66

Figura 31. Mostrar las coincidencias recibidas luego de ser establecida en R2. ...	68
Figura 32. Restablecer los contadores de una lista de acceso. ....	68
Figura 33. Mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica. ....	69
Figura 34. Mostrar las traducciones NAT. ....	69
Figura 35. Comando utilizado para eliminar las traducciones de NAT dinámicas. ....	70

## GLOSARIO

**ACL:** Una lista de control de acceso (ACL) es filtros de tráfico de una lista de redes y acciones correlacionadas usados para mejorar la Seguridad. Bloquea o permite que los usuarios accedan los recursos específicos.

**LAN:** Una red local es la interconexión de varios computadores y periféricos. Su extensión está limitada físicamente a un edificio o a un entorno de unos pocos kilómetros.

**NAT:** La traducción de direcciones de red, también llamado enmascaramiento de IP o NAT, es un mecanismo utilizado por routers IP para cambiar paquetes entre dos redes que asignan mutuamente direcciones incompatibles. Consiste en convertir, en tiempo real, las direcciones utilizadas en los paquetes transportados.

**NTP:** Network Time Protocol (NTP) es un protocolo de Internet para sincronizar los relojes de los sistemas informáticos a través del enrutamiento de paquetes en redes con latencia variable.

**OSPF:** Open Shortest Path First, Abrir el camino más corto primero en español, es un protocolo de red para encaminamiento jerárquico de pasarela interior o Interior Gateway Protocol, que usa el algoritmo Dijkstra, para calcular la ruta más corta entre dos nodos.

**ROUTER:** Dispositivo hardware o software de interconexión de redes de computadores que opera en la capa tres (nivel de red) del modelo OSI. Este dispositivo interconecta segmentos de red o redes enteras.

**SWITCH:** Dispositivo de interconexión de redes de computadores que opera en la capa 2 (nivel de enlace de datos) del modelo OSI (Open Systems Interconnection). Un switch interconecta dos o más segmentos de red, pasando datos de un segmento a otro, de acuerdo con la dirección de destino de los datagramas en la red.

**VLAN basado en protocolos:** Los grupos basados en protocolos pueden ser definidos y estar limitados a un puerto; por lo tanto, cada paquete que origina de los grupos de protocolos se asigna al VLAN configurado en la página. El VLAN basado en protocolos divide la red física en los grupos VLAN lógicos para cada protocolo requerido.



## RESUMEN

La evaluación denominada “Prueba de habilidades prácticas”, forma parte de las actividades evaluativas del Diplomado de Profundización CCNA, y busca identificar el grado de desarrollo de competencias y habilidades que fueron adquiridas a lo largo del diplomado. Lo esencial es poner a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos de Networking.

PALABRAS CLAVE: CISCO, Conmutación, Enrutamiento, Redes, Sistemas.

## ABSTRACT

The evaluation called "Test of practical skills" is part of the evaluative activities of the CCNA Deepening Diploma, and seeks to identify the degree of development of skills and abilities that were acquired throughout the diploma. The essential thing is to test the levels of understanding and problem solving related to various aspects of Networking.

KEY WORDS: CISCO, Switching, Routing, Networks, Systems.

## INTRODUCCIÓN

La evaluación denominada “Prueba de habilidades prácticas”, forma parte de las actividades evaluativas del Diplomado de Profundización CCNA, y busca identificar el grado de desarrollo de competencias y habilidades que fueron adquiridas a lo largo del diplomado. Lo esencial es poner a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos de Networking.

Para esta actividad, el estudiante dispone de cerca de dos semanas para realizar las tareas asignadas en cada uno de los dos (2) escenarios propuestos, acompañado de los respectivos procesos de documentación de la solución, correspondientes al registro de la configuración de cada uno de los dispositivos, la descripción detallada del paso a paso de cada una de las etapas realizadas durante su desarrollo, el registro de los procesos de verificación de conectividad mediante el uso de comandos ping, traceroute, show ip route, entre otros.

Teniendo en cuenta que la Prueba de habilidades está conformada por dos (2) escenarios, el estudiante deberá realizar el proceso de configuración de usando cualquiera de las siguientes herramientas: Packet Tracer o GNS3.

## DESARROLLO

### 1. ESCENARIO 1

Topología.

Figura 1. Topología propuesta para el escenario 1.



Fuente: Autor.

En este primer escenario se configurarán los dispositivos de una red pequeña. Debe configurar un router, un switch y equipos, diseñar el esquema de direccionamiento IPv4 para las LAN propuestas. El router y el switch también deben administrarse de forma segura.

#### Objetivos

Parte 1: Construir en el simulador la Red

Parte 2: Desarrollar el esquema de direccionamiento IP para la LAN1 y la LAN2

Parte 3: Configurar los aspectos básicos de los dispositivos de la Red propuesta.

Parte 4: Configurar los ajustes básicos de seguridad en el R1 y S1

Parte 4: Configurar los hosts y verificar la conectividad entre los equipos

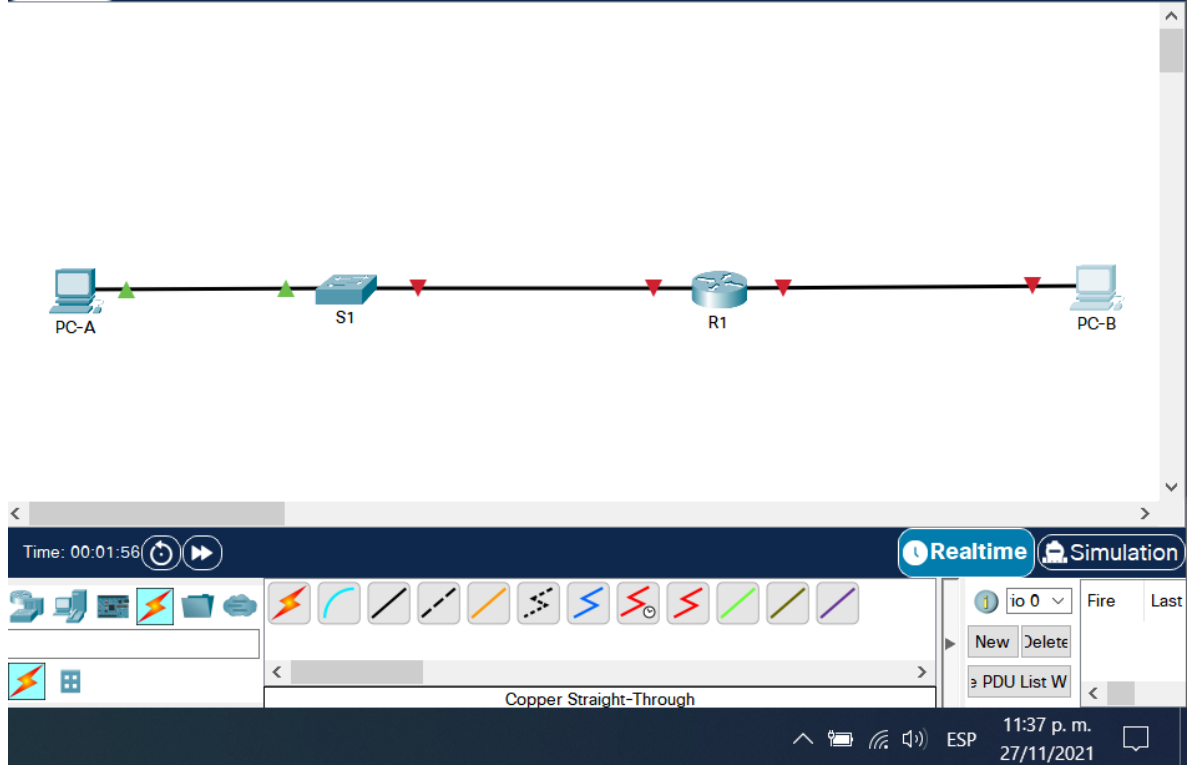
#### Aspectos básicos/situación.

En el desarrollo del caso de estudio usted implementa la topología mostrada en la figura y configura el Router R1 y el switch S1, y los PCs. Con la dirección suministrada realizará el subnetting y cumplirá el requerimiento para la LAN1 (100 host) y la LAN2 (50 hosts).

#### Parte 1: Construya la Red

En el simulador construya la red de acuerdo con la topología lógica que se plantea en la figura 1, cablee conforme se indica en la topología, y conecte los equipos de cómputo.

Figura 2. Presentación de la topología en packet tracer.



Fuente: Autor.

## Parte 2: Desarrolle el esquema de direccionamiento IP

Desarrolle el esquema de direccionamiento IP. Para la dirección IPv4 cree las dos subredes con la cantidad requerida de hosts. Asigne las direcciones de acuerdo con los requisitos mencionados en la tabla de direccionamiento.

Cada estudiante tomará el direccionamiento 192.168.X.0 donde X corresponde a los últimos dos dígitos de su cédula.

Tabla 1. Tabla de direccionamiento LAN1.

Dirección de subred	192.168.69.0	
Gateway	192.168.69.1	255.255.255.128
1er Host	192.168.69.2	255.255.255.128
Último Host	192.168.69.126	255.255.255.128
Broadcast	192.168.69.127	255.255.255.128

Fuente: Autor.

Tabla 2. Tabla de direccionamiento LAN2.

Dirección de subred	192.168.69.128	
Gateway	192.168.69.129	255.255.255.192
1er Host	192.168.69.130	255.255.255.192
Último Host	192.168.69.190	255.255.255.192
Broadcast	192.168.69.191	255.255.255.192

Fuente: Autor.

Tabla 3. Tabla de direccionamiento para el primer escenario.

Item	Requerimiento
Dirección de red	192.168.69.0
Requerimiento de host Subred LAN1	100
Requerimiento de host Subred LAN2	50
R1 G0/0/1	192.168.69.1
R1 G0/0/0	192.168.69.129
S1 SVI	192.168.69.3
PC-A	192.168.69.126
PC-B	192.168.69.190

Fuente: Autor.

### Parte 3: Configure aspectos básicos

Los dispositivos de red (S1 y R1) se configuran mediante conexión de consola.

Paso 1: configurar los ajustes básicos.

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 4. Lista de configuraciones para aplicar en R1.

Tarea	Especificación
Desactivar la búsqueda DNS	
Nombre del router	R1
Nombre de dominio	ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	ciscoenpass
Contraseña de acceso a la consola	ciscoconpass
Establecer la longitud mínima para las contraseñas	10 caracteres
Crear un usuario administrativo en la base de datos local	Nombre de usuario: <b>admin</b> Password: <b>admin1pass</b>
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	



R1(config-line)#login local use la base de datos local.	Se configura para que
R1(config-line)#transport input ssh transporte por la línea solo ssh	Se habilita el
R1(config-line)#exit	
R1(config)#interface gi0/0/1 interfaz gi0/0	Se accede a la
R1(config-if)#description LAN1 descripción a la interfaz.	Se configura una
R1(config-if)#ip add 192.168.45.1 255.255.255.128 direccionamiento a la interfaz	Se configura el
R1(config-if)#no shutdown gi0/0	Se activa la interfaz
R1(config-if)#exit	
R1(config)#interface gi0/0/0 interfaz	Se accede a la
R1(config-if)#description LAN2 descripción a la interfaz	Se configura una
R1(config-if)#ip add 192.168.45.129 255.255.255.192 direccionamiento a la interfaz	Se configura el
R1(config-if)#no shutdown gi1/0	Se activa la interfaz
R1(config-if)#exit	
R1(config)#service password-encryption contraseñas.	Cifrado de las
R1(config)# banner motd #El acceso sin permiso queda prohibido# banner que muestra un mensaje de advertencia.	Se añade un

Las tareas de configuración de S1 incluyen lo siguiente:

Tabla 5. Tabla de configuraciones en S1.

Tarea	Especificación
Desactivar la búsqueda DNS.	
Nombre del switch	<b>S1</b>
Nombre de dominio	<b>ccna-lab.com</b>
Contraseña cifrada para el modo EXEC privilegiado	<b>ciscoenpass</b>
Contraseña de acceso a la consola	<b>ciscoconpass</b>



Crear un usuario administrativo en la base de datos local	<b>Nombre de usuario: admin</b> <b>Password: admin1pass</b>
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	
Cifrar las contraseñas de texto no cifrado	
Configurar un MOTD Banner	
Generar una clave de cifrado RSA	<b>Módulo de 1024 bits</b>
Configurar la interfaz de administración (SVI)	Establecer la dirección IPv4 de capa 3 conforme la tabla de direccionamiento
Configuración del gateway predeterminado	Configure la puerta de enlace predeterminada conforme a la tabla de direccionamiento.

Fuente: Autor.

## Switch S1

Switch#configure terminal	
Switch (config)#hostname S1	Se configura el
nombre del dispositivo	
S1(config)#no ip domain-lookup	Se desactiva la
búsqueda de dominio	
S1(config)#ip domain-name ccna-lab.com	Se configura un
nombre de dominio	
S1(config)#enable secret ciscoenpass	Se configura una
contraseña de exec secreta	
S1(config)#line con 0	Se ingresa a la línea
de consola	
S1(config-line)#password ciscoconpass	Se configura una
contraseña a la línea de consola	
S1(config-line)#login	Se habilita la revisión
de la contraseña	
S1(config-line)#exit	
S1(config)#username admin password admin1pass	Se crea un usuario
administrativo	
S1(config)#crypto key generate rsa	Se genera una clave
de cifrado RSA de 1024 bits	
S1(config)#ip ssh version 2	Se habilita ip ssh
versión 2	

S1(config)#line vty 0 4 de terminal	Se accede a la línea
S1(config-line)#login local use la base de datos local	Se configura para que
S1(config-line)#transport input ssh transporte por la línea solo ssh	Se habilita el
S1(config-line)#exit	
S1(config)#service password-encryption contraseñas.	Cifrado de las
S1(config)#banner motd # El acceso sin permiso queda prohibido # Se configura un mensaje de advertencia	
S1(config)#interface vlan 1 interfaz vlan	Se accede a la
S1(config-if)# description SVI del Switch S1 descripción a la SVI	Se configura una
S1(config-if)#ip add 192.168.45.2 255.255.255.128 dirección ip de capa 3.	Se configura una
S1(config-if)#no shutdown interfaz	Se enciende la
S1(config-if)#exit	
S1(config)#ip default-gateway 192.168.45.1 dirección de puerta de enlace predeterminada en S1	Se configura la
S1(config)#	

## Paso 2. Configurar los equipos

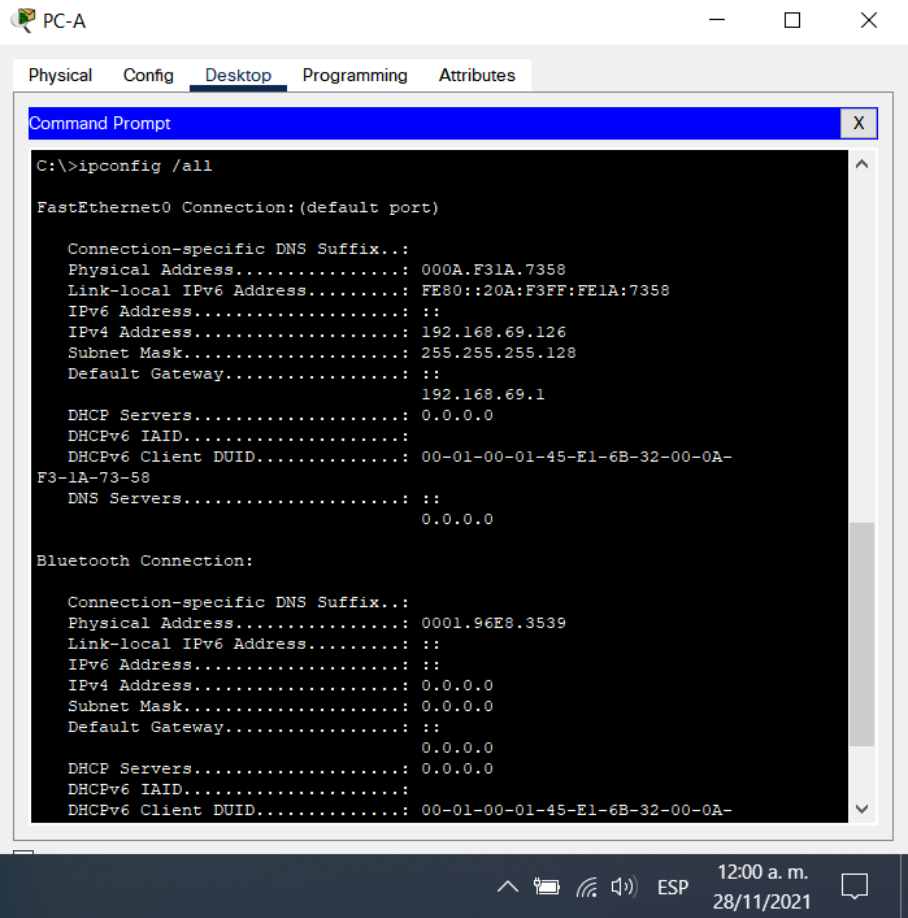
Configure los equipos host PC-A y PC-B conforme a la tabla de direccionamiento, registre las configuraciones de red del host con el comando ipconfig /all.

Tabla 6. Configuración de direccionamiento en PC-A.

PC-A Network Configuration	
Descripción	PC-A
Dirección física	000A.F31A.7358
Dirección IP	192.168.69.126
Máscara de subred	255.255.255.128
Gateway predeterminado	192.168.69.1

Fuente: Autor.

Figura 3. Configuraciones de red del host con el comando ipconfig /all en PC-A.



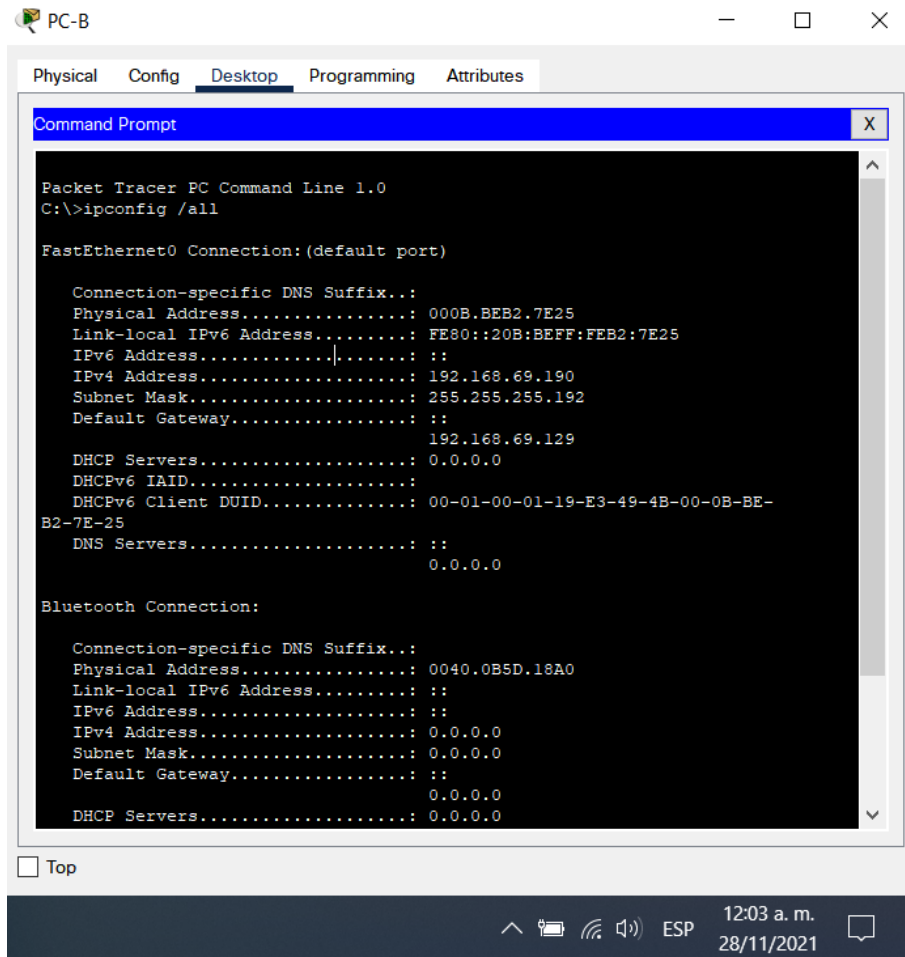
Fuente: Autor.

Tabla 7. Configuración de direccionamiento en PC-B.

PC-B Network Configuration	
Descripción	PC-B
Dirección física	000B.BEB2.7E25
Dirección IP	192.168.69.190
Máscara de subred	255.255.255.192
Gateway predeterminado	192.168.69.129

Fuente: Autor.

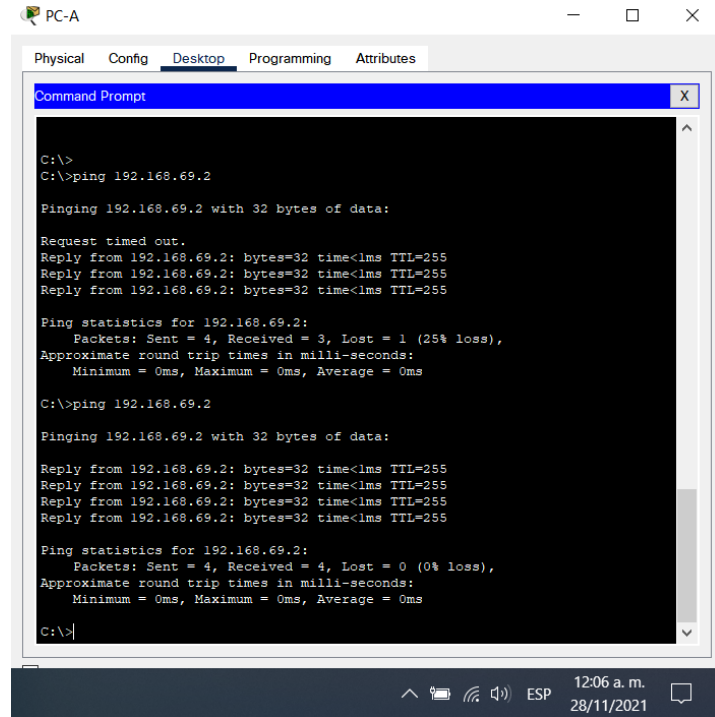
Figura 4. Evidencia de la configuración del PC-B.



Fuente: Autor.

Luego de realizada la configuración de los host PC-A y PC-B, se procede a realizar una prueba de conectividad entre ellos, esta se presenta a continuación:

Figura 5. Prueba de conectividad entre PC-A y SVI del switch S1.



```
PC-A
Physical Config Desktop Programming Attributes
Command Prompt
C:\>
C:\>ping 192.168.69.2

Pinging 192.168.69.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.69.2: bytes=32 time<1ms TTL=255
Reply from 192.168.69.2: bytes=32 time<1ms TTL=255
Reply from 192.168.69.2: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.69.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.69.2

Pinging 192.168.69.2 with 32 bytes of data:

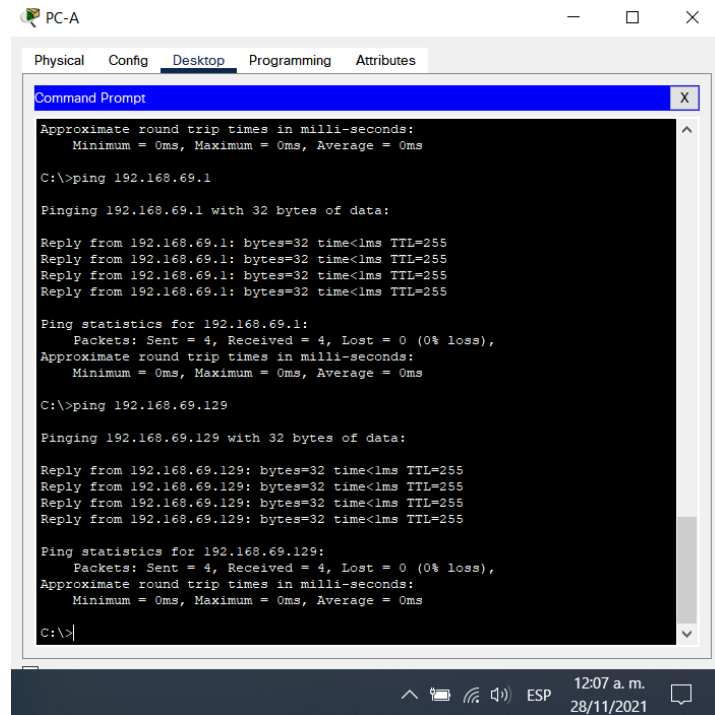
Reply from 192.168.69.2: bytes=32 time<1ms TTL=255
Reply from 192.168.69.2: bytes=32 time<1ms TTL=255
Reply from 192.168.69.2: bytes=32 time<1ms TTL=255
Reply from 192.168.69.2: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.69.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>|
```

Fuente: Autor.

Figura 6. Prueba de conectividad entre PC-A y las interfaces de R1.



```
PC-A
Physical Config Desktop Programming Attributes
Command Prompt
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 192.168.69.1

Pinging 192.168.69.1 with 32 bytes of data:

Reply from 192.168.69.1: bytes=32 time<1ms TTL=255
Reply from 192.168.69.1: bytes=32 time<1ms TTL=255
Reply from 192.168.69.1: bytes=32 time<1ms TTL=255
Reply from 192.168.69.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.69.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.69.129

Pinging 192.168.69.129 with 32 bytes of data:

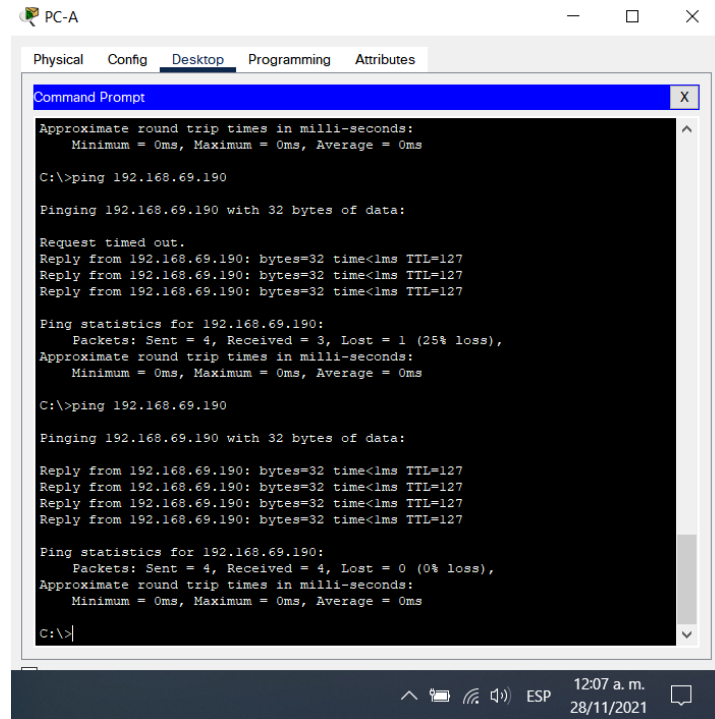
Reply from 192.168.69.129: bytes=32 time<1ms TTL=255
Reply from 192.168.69.129: bytes=32 time<1ms TTL=255
Reply from 192.168.69.129: bytes=32 time<1ms TTL=255
Reply from 192.168.69.129: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.69.129:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>|
```

Fuente: Autor.

Figura 7. Prueba de conectividad entre PC-A y PC-B.



```
PC-A
Physical Config Desktop Programming Attributes
Command Prompt
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.69.190

Pinging 192.168.69.190 with 32 bytes of data:

Request timed out.
Reply from 192.168.69.190: bytes=32 time<1ms TTL=127
Reply from 192.168.69.190: bytes=32 time<1ms TTL=127
Reply from 192.168.69.190: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.69.190:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.69.190

Pinging 192.168.69.190 with 32 bytes of data:

Reply from 192.168.69.190: bytes=32 time<1ms TTL=127
Reply from 192.168.69.190: bytes=32 time<1ms TTL=127
Reply from 192.168.69.190: bytes=32 time<1ms TTL=127
Reply from 192.168.69.190: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.69.190:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>|
```

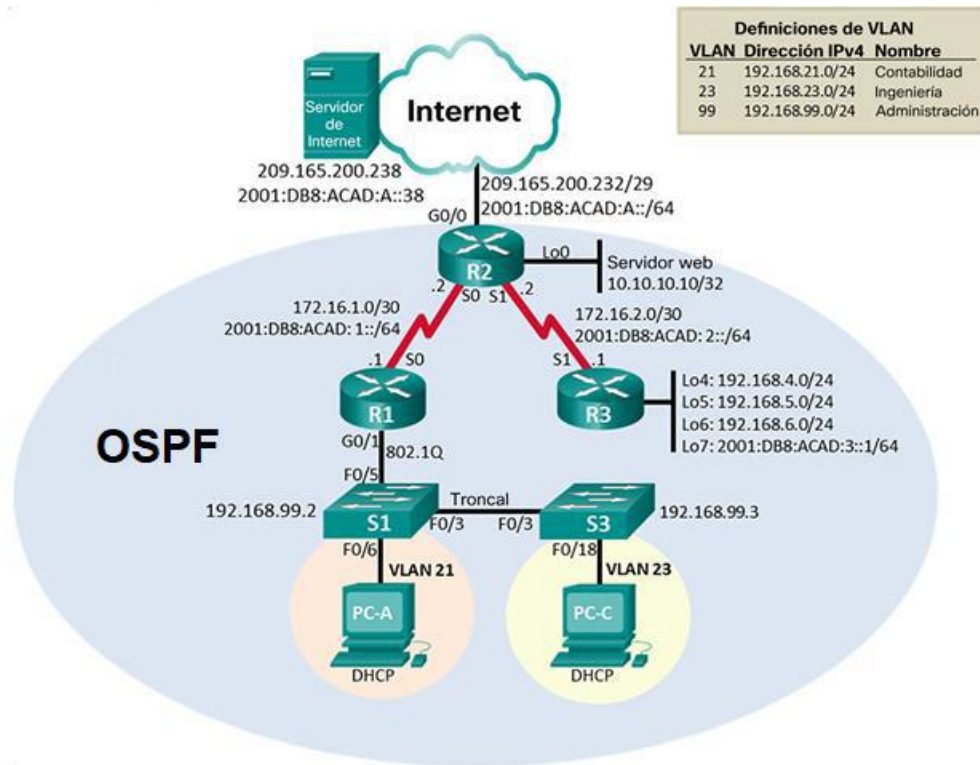
Fuente: Autor.

## 2. ESCENARIO 2

Escenario: Se debe configurar una red pequeña para que admita conectividad IPv4 e IPv6, seguridad de switches, routing entre VLAN, el protocolo de routing dinámico OSPF, el protocolo de configuración de hosts dinámicos (DHCP), la traducción de direcciones de red dinámicas y estáticas (NAT), listas de control de acceso (ACL) y el protocolo de tiempo de red (NTP) servidor/cliente. Durante la evaluación, probará y registrará la red mediante los comandos comunes de CLI.

# Topología

Figura 8. Topología propuesta para el escenario 2.



Fuente: Autor.

## Parte 1: Inicializar dispositivos

## Paso 1: Inicializar y volver a cargar los routers y los switches

Elimine las configuraciones de inicio y vuelva a cargar los dispositivos.

Antes de continuar, solicite al instructor que verifique la inicialización de los dispositivos.

Tabla 8. Tabla de configuraciones para inicializar y volver a cargar los routers y los switches.

<b>Tarea</b>	<b>Comando de IOS</b>
Eliminar el archivo startup-config de todos los routers	
Volver a cargar todos los routers	
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	
Volver a cargar ambos switches	
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	

Fuente: Autor.

#### Router R1

R1#erase startup-config	Este comando elimina
el archivo startup-config	
R1#reload	Este comando
permite volver a cargar el dispositivo	

#### Router R2

R2#erase startup-config	Este comando elimina
el archivo startup-config	
R2#reload	Este comando
permite volver a cargar el dispositivo	

#### Configuración en R3

R3#erase startup-config	Este comando elimina
el archivo startup-config	
R3#reload	Este comando
permite volver a cargar el dispositivo	



## Configuración en S1

S1#erase startup-config

Este comando elimina

el archivo startup-config

S1#reload

Este

comando

permite volver a cargar el dispositivo

## Configuración en S3

S3#erase startup-config

Este comando elimina

el archivo startup-config

S3#reload

Este

comando

permite volver a cargar el dispositivo

Figura 9. Verificación de que la base de datos de VLAN no esté en la memoria flash en S1

```
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE4,
RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2013 by Cisco Systems, Inc.
Compiled Wed 26-Jun-13 02:49 by mnguyen

Press RETURN to get started!

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed
state to up
%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6, changed
state to up

Switch>enable
Switch#show flash:
Directory of flash:

 1  -rw-   4670455    <no date>  2960-lanbasek9-mz.150-2.SE4.bin

64016384 bytes total (59345929 bytes free)
Switch#
```

Fuente: Autor.

Figura 10. Verificación de que la base de datos de VLAN no esté en la memoria flash en S2

```

Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE4,
RELEASE SOFTWARE (fcl)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2013 by Cisco Systems, Inc.
Compiled Wed 26-Jun-13 02:49 by mnguyen

Press RETURN to get started!

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed
state to up
%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/18, changed
state to up

Switch>enable
Switch#show flash:
Directory of flash:/

 1  -rw-   4670455      <no date>  2960-lanbasek9-mz.150-2.SE4.bin

64016384 bytes total (59345929 bytes free)
Switch#
  
```

Fuente: Autor.

## Parte 2: Configurar los parámetros básicos de los dispositivos

### Paso 1: Configurar la computadora de Internet

Las tareas de configuración del servidor de Internet incluyen lo siguiente (para obtener información de las direcciones IP, consulte la topología):

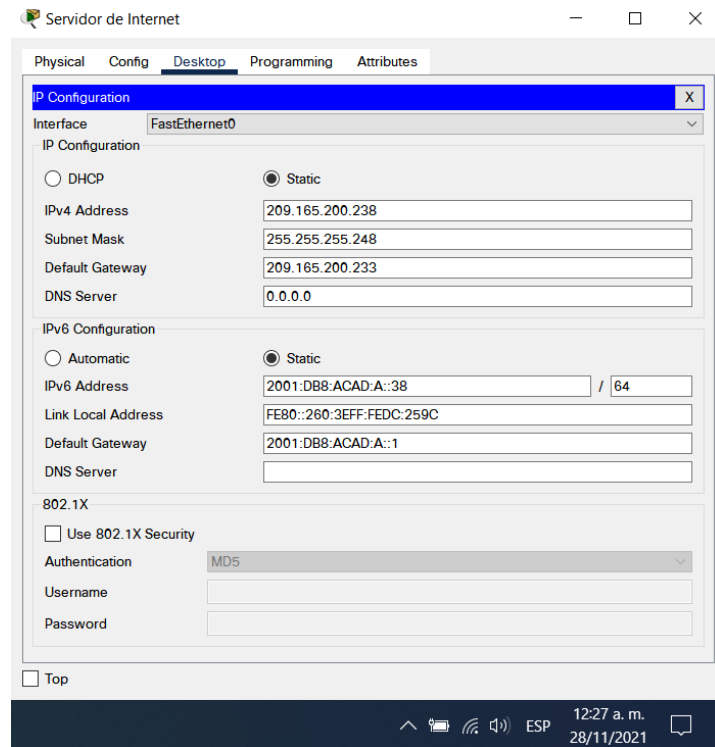
Tabla 9. Configuración de la computadora de Internet.

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.233
Dirección IPv6/subred	2001:DB8:ACAD:A::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:A::1

Fuente: Autor.

Nota: Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente en partes posteriores de esta práctica de laboratorio.

Figura 11. Configuración del Servidor de Internet.



Fuente: Autor.

## Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 10. Configuración de R1.

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	No ip domain-lookup
Nombre del router	R1
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	Service password-encryption

Mensaje MOTD	Se prohíbe el acceso no autorizado.
Interfaz S0/0/0	Establezca la descripción Establecer la dirección IPv4 Consultar el diagrama de topología para conocer la información de direcciones Establecer la dirección IPv6 Consultar el diagrama de topología para conocer la información de direcciones Establecer la frecuencia de reloj en 128000 Activar la interfaz
Rutas predeterminadas	Configurar una ruta IPv4 predeterminada de S0/0/0 Configurar una ruta IPv6 predeterminada de S0/0/0

Fuente: Autor.

Nota: Todavía no configure G0/1.

#### Router R1

R1#configure terminal	
R1(config)#no ip domain-lookup	Se desactiva la
búsqueda de dominio	
R1(config)#hostname R1	Se configura un
nombre de host a R1	
R1(config)#enable secret class	Se asigna la
contraseña de exec privilegiado cifrada	
R1(config)#line con 0	Se accede a la línea
de consola	
R1(config-line)#password cisco	Se configura la clave
de consola	
R1(config-line)#login	Se habilita la
validación de contraseña	
R1(config-line)#exit	
R1(config)#line vty 0 4	Se accede a la línea
telnet	
R1(config-line)#password cisco	Se configura la clave
de telnet	

R1(config-line)#login	Se	habilita	la
validación de contraseña telnet			
R1(config-line)#exit			
R1(config)#service password-encryption	Se	activa	el servicio
de encriptación de contraseñas			
R1(config)#banner motd # El acceso sin permiso queda prohibido #	Se	agrega	un
mensaje de advertencia			
R1(config)#interface se0/0/0	Se	accede	a la
interfaz serial1/0			
R1(config-if)#description WAN a R2	Se	configura	la
descripción a la interfaz serial			
R1(config-if)#ip add 172.16.1.1 255.255.255.252	Se	configura	la
dirección ipv4.			
R1(config-if)#ipv6 add 2001:db8:acad:1::1/64	Se	configura	la
dirección ipv6			
R1(config-if)#clock rate 128000	Se	establece	la
velocidad de la conexión serial.			
R1(config-if)#no shutdown	Se	enciende	la
interfaz			
R1(config-if)#exit			
R1(config)#ip route 0.0.0.0 0.0.0.0 se0/0/0	Se	configura	una ruta
estática predeterminada ipv4			
R1(config)#ipv6 route ::/0 se1/0	Se	configura	una ruta
estática predeterminada ipv6			
R1(config)#ipv6 unicast-routing	Se	habilita	el
enrutamiento para IPv6			

### Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Tabla 11. Configuración de R2.

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	No ip domain-lookup
Nombre del router	R2
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco

Cifrar las contraseñas de texto no cifrado	Service password-encryption
Habilitar el servidor HTTP	Ip http server
Mensaje MOTD	Se prohíbe el acceso no autorizado.
Interfaz S0/0/0	Establezca la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz
Interfaz S0/0/1	Establecer la descripción Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Establecer la frecuencia de reloj en 128000. Activar la interfaz
Interfaz G0/0 (simulación de Internet)	Establecer la descripción. Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Establezca la dirección IPv6. Utilizar la primera dirección disponible en la subred. Activar la interfaz
Interfaz loopback 0 (servidor web simulado)	Establecer la descripción. Establezca la dirección IPv4.
Ruta predeterminada	Configure una ruta IPv4 predeterminada de G0/0. Configure una ruta IPv6 predeterminada de G0/0.

Fuente: Autor.

Router R2

R2#configure terminal

R2(config)#no ip domain-lookup  
búsqueda de dominio

Se desactiva la

R2(config)#hostname R2 nombre de host	Se configura el
R2(config)#enable secret class contraseña de EXEC	Se configura la
R2(config)#line con 0 R2(config-line)#password cisco contraseña de consola	Se configura la
R2(config-line)#login verificación de contraseña de consola	Se habilita la
R2(config-line)#exit R2(config)#line vty 0 4 R2(config-line)#password cisco contraseña de terminal de acceso telnet	Se configura la
R2(config-line)#login verificación de contraseña de acceso telnet	Se habilita la
R2(config-line)#exit R2(config)#service password-encryption de encriptación de contraseñas de texto plano	Se habilita el servicio
R2(config)#ip http server	Se activa el servidor
R2(config)#banner motd # El acceso sin permiso queda prohibido # mensaje de advertencia	Se habilita un
R2(config)#interface se0/0/0 R2(config-if)#description WAN a R1 descripción de la interfaz	Se configura la
R2(config-if)#ip add 172.16.1.2 255.255.255.252 direccionamiento de la interfaz	Se configura el
R2(config-if)#ipv6 add 2001:db8:acad:1::2/64 direccionamiento IPv6 de la interfaz	Se configura el
R2(config-if)#no shutdown interfaz	Se enciende la
R2(config-if)#exit R2(config)#interface se0/0/1 R2(config-if)#description WAN a R3 descripción de la interfaz	Se configura la
R2(config-if)#ip add 172.16.2.2 255.255.255.252 direccionamiento de la interfaz	Se configura el
R2(config-if)#ipv6 add 2001:DB8:ACAD:2::2/64 direccionamiento IPv6 de la interfaz	Se configura el

R2(config-if)#clock rate 128000 velocidad de la sincronización	Se	configura	la
R2(config-if)#no shutdown interfaz	Se	enciende	la
R2(config-if)#exit R2(config)#interface gi0/0			
R2(config-if)#description Simulacion de Internet descripción de la interfaz	Se	configura	la
R2(config-if)#ip add 209.165.200.233 255.255.255.248 direccionamiento de la interfaz	Se	configura	el
R2(config-if)#ipv6 add 2001:DB8:ACAD:A::1/64 direccionamiento IPv6 de la interfaz	Se	configura	el
R2(config-if)#no shutdown interfaz	Se	enciende	la
R2(config-if)#exit R2(config)#interface lo0			
R2(config-if)#description Servidor Web Simulado descripción de la interfaz loopback	Se	configura	la
R2(config-if)#ip add 10.10.10.10 255.255.255.255 direccionamiento de la interfaz	Se	configura	el
R2(config-if)#no shutdown interfaz	Se	enciende	la
R2(config-if)#exit R2(config)#ip route 0.0.0.0 0.0.0.0 gi0/0 predeterminada para el direccionamiento	Se	asigna	una ruta
R2(config)#ipv6 route ::/0 gi0/0 predeterminada para el direccionamiento	Se	configura	una ruta
R2(config)#ipv6 unicast-routing enrutamiento para IPv6	Se	habilita	el

#### Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Tabla 12. Configuración de R3.

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	No ip domain-lookup
Nombre del router	R3



Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	Service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado.
Interfaz S0/0/1	Establecer la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz
Interfaz loopback 4	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
Interfaz loopback 5	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
Interfaz loopback 6	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
Interfaz loopback 7	Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.
Rutas predeterminadas	Configure una ruta IPv4 e IPv6 predeterminada en la interface S0/0/1

Fuente: Autor.

### Router R3

R3#configure terminal	
R3(config)#no ip domain-lookup	Se desactiva la
búsqueda de dominio	
R3(config)#hostname R3	Se configura el
nombre de host	
R3(config)#enable secret class	Se configura la
contraseña de EXEC	
R3(config)#line con 0	

R3(config-line)#password cisco contraseña de consola	Se configura la
R3(config-line)#login verificación de contraseña de consola	Se habilita la
R3(config-line)#exit	
R3(config)#line vty 0 4	
R3(config-line)#password cisco contraseña de terminal de acceso telnet	Se configura la
R3(config-line)#login verificación de contraseña de acceso telnet	Se habilita la
R3(config-line)#exit	
R3(config)#service password-encryption de encriptación de contraseñas de texto plano	Se habilita el servicio
R3(config)#banner motd # El acceso sin permiso queda prohibido #	Se habilita un mensaje de advertencia
R3(config)#interface se0/0/1	
R3(config-if)#description WAN a R2 descripción de la interfaz	Se configura la
R3(config-if)#ip add 172.16.2.1 255.255.255.252 direccionamiento de la interfaz	Se configura el
R3(config-if)#ipv6 add 2001:DB8:ACAD:2::1/64 direccionamiento IPv6 de la interfaz	Se configura el
R3(config-if)#no shutdown	Se activa la interfaz
R3(config-if)#exit	
R3(config)#interface lo4 descripción de la interfaz loopback	Se configura la
R3(config-if)#ip add 192.168.4.1 255.255.255.0 direccionamiento de la interfaz	Se configura el
R3(config-if)#exit	
R3(config)#interface lo5 descripción de la interfaz loopback	Se configura la
R3(config-if)#ip add 192.168.5.1 255.255.255.0 direccionamiento de la interfaz	Se configura el
R3(config-if)#exit	
R3(config)#interface lo6 descripción de la interfaz loopback	Se configura la
R3(config-if)#ip add 192.168.6.1 255.255.255.0 direccionamiento de la interfaz	Se configura el
R3(config-if)#exit	

R3(config)#interface lo7	Se configura la
descripción de la interfaz loopback	
R3(config-if)#ipv6 add 2001:db8:acad:3::1/64	Se configura el
direccionamiento de la interfaz	
R3(config-if)#exit	
R3(config)#ip route 0.0.0.0 0.0.0.0 se0/0/1	Se configura una ruta
predeterminada para el direccionamiento IPv4 en la interfaz Se0/0/1	
R3(config)#ipv6 route ::/0 se0/0/1	Se configura una ruta
predeterminada para el direccionamiento IPv6 en la interfaz Se0/0/1	
R3(config)#ipv6 unicast-routing	Se habilita el
enrutamiento para IPv6	

### Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 13. Configuración de S1.

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	No ip domain-lookup
Nombre del switch	S1
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	Service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado.

Fuente: Autor.

### Switch S1

S1#configure terminal	
S1(config)#no ip domain-lookup	Se desactiva la
búsqueda de dominio	
S1(config)#hostname S1	Se configura el
nombre de host	
S1(config)#enable secret class	Se configura la
contraseña de EXEC	
S1(config)#line con 0	

S1(config-line)#password cisco	Se	configura	la
contraseña de consola			
S1(config-line)#login	Se	habilita	la
verificación de contraseña de consola			
S1(config-line)#exit			
S1(config)#line vty 0 15			
S1(config-line)#password cisco	Se	configura	la
contraseña de terminal de acceso telnet			
S1(config-line)#login	Se	habilita	la
verificación de contraseña de acceso telnet			
S1(config-line)#exit			
S1(config)#service password-encryption	Se	habilita	el servicio
de encriptación de contraseñas de texto plano			
S1(config)#banner motd # El acceso sin permiso queda prohibido #	Se	habilita	un
mensaje de advertencia			

#### Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 14. Configuración de S3.

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	No ip domain-lookup
Nombre del switch	S3
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	Service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado.

Fuente: Autor.

#### Switch S3

S3#configure terminal			
S3(config)#no ip domain-lookup	Se	desactiva	la
búsqueda de dominio			

S3(config)#hostname S3 nombre de host	Se configura el
S3(config)#enable secret class contraseña de EXEC	Se configura la
S3(config)#line con 0 S3(config-line)#password cisco contraseña de consola	Se configura la
S3(config-line)#login verificación de contraseña de consola	Se habilita la
S3(config-line)#exit S3(config)#line vty 0 15 S3(config-line)#password cisco contraseña de terminal de acceso telnet	Se configura la
S3(config-line)#login verificación de contraseña de acceso telnet	Se habilita la
S3(config-line)#exit S3(config)#service password-encryption de encriptación de contraseñas de texto plano	Se habilita el servicio
S3(config)#banner motd # El acceso sin permiso queda prohibido # mensaje de advertencia	Se habilita un
S3(config)#	

#### Paso 7: Verificar la conectividad de la red

Utilice el comando ping para probar la conectividad entre los dispositivos de red.

Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

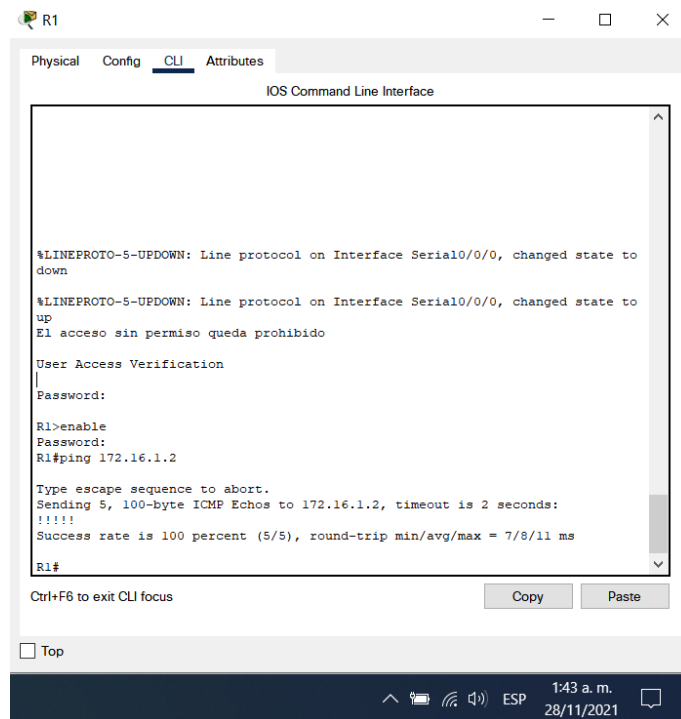
Tabla 15. Verificación de la conectividad de la red.

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds: !!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 7/8/11 ms
R2	R3, S0/0/1	172.16.2.1	Sending 5, 100-byte ICMP Echos to 172.16.2.1, timeout is 2 seconds: !!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 8/8/10 ms
PC de Internet	Gateway predeterminado	209.165.200.233	C:\>ping 209.165.200.233  Pinging 209.165.200.233 with 32 bytes of data:  Reply from 209.165.200.233: bytes=32 time<1ms TTL=255 Reply from 209.165.200.233: bytes=32 time<1ms TTL=255 Reply from 209.165.200.233: bytes=32 time<1ms TTL=255 Reply from 209.165.200.233: bytes=32 time<1ms TTL=255  Ping statistics for 209.165.200.233: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms

Fuente: Autor.

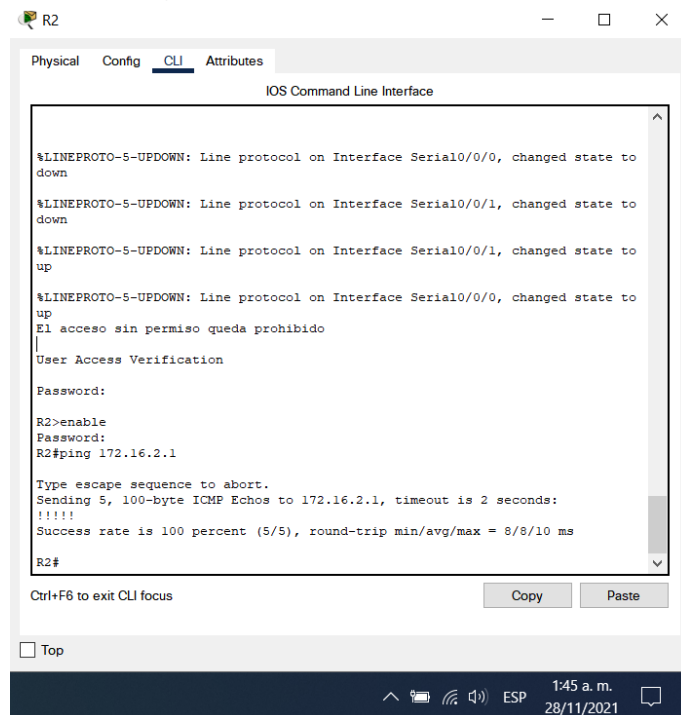
Nota: Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

Figura 12. Validación de ping desde R1 a R2.



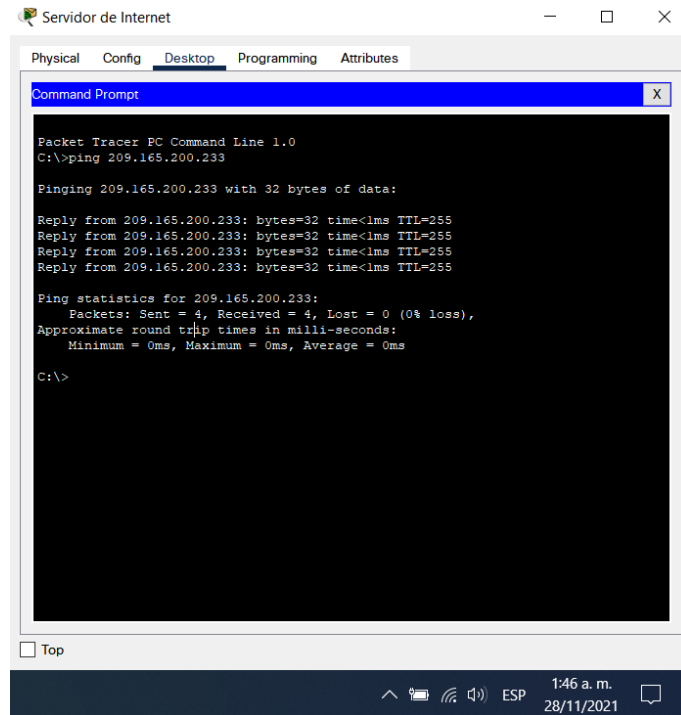
Fuente: Autor

Figura 13. Validación de ping desde R2 a R3.



Fuente: Autor

Figura 14. Validación de ping desde Servidor de Internet a su Gateway.



Fuente: Autor.

### Parte 3: Configurar la seguridad del switch, las VLAN y el routing entre VLAN

#### Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 16. Tabla de configuración de seguridad, VLAN y routing entre VLAN en S1.

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear y nombrar cada una de las VLAN que se indican
Asignar la dirección IP de administración.	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S1 en el diagrama de topología
Asignar el gateway predeterminado	Asigne la primera dirección IPv4 de la subred como el gateway predeterminado.



Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa
Forzar el enlace troncal en la interfaz F0/5	Utilizar la red VLAN 1 como VLAN nativa
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range
Asignar F0/6 a la VLAN 21	
Apagar todos los puertos sin usar	

Fuente: Autor.

## Switch S1

S1(config)#vlan 21 VLAN21	Se configura la
S1(config-vlan)#name Contabilidad nombre de la VLAN	Se configura el
S1(config-vlan)#exit	
S1(config)#vlan 23 VLAN23	Se configura la
S1(config-vlan)#name Ingenieria nombre de la VLAN	Se configura el
S1(config-vlan)#exit	
S1(config)#vlan 99 VLAN99	Se configura la
S1(config-vlan)#name Administracion nombre de la VLAN	Se configura el
S1(config-vlan)#exit	
S1(config)#	
S1(config)#interface vlan 99 de la VLAN 99	Se habilita la interfaz
S1(config-if)#ip add 192.168.99.2 255.255.255.0 direccionamiento de la interfaz	Se configura el
S1(config-if)#no shutdown interfaz	Se enciende la
S1(config-if)#exit	
S1(config)#ip default-gateway 192.168.99.1 dirección de la puerta de acceso por defecto	Se configura la
S1(config)#interface range fa0/5, fa0/3 interfaces que son puertas troncales	Se seleccionan las

S1(config-if-range)#switchport mode trunk truncal	Se configura en modo
S1(config-if-range)#switchport trunk native vlan 1 como vlan nativa	Se habilita la VLAN 1
S1(config-if-range)#exit S1(config)#interface fa0/6	
S1(config-if)#switchport mode access interfaz con modo de acceso	Se configura la
S1(config-if)#switchport access vlan 21 21 para que circule en esta interfaz	Se configura la VLAN
S1(config-if)#exit S1(config)# interface range fa0/1-2,fa0/4,fa0/7-24,gi0/1-2	Se seleccionan las
interfases que están inactivas	
S1(config-if-range)#switchport mode Access modo de acceso	Se configuran en
S1(config-if-range)#shutdown S1(config-if-range)#exit	Se desactivan las interfaces.

## Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 17. Tabla de configuración de seguridad, VLAN y routing entre VLAN en S3.

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear cada una de las VLAN que se indican Dé nombre a cada VLAN.
Asignar la dirección IP de administración	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S3 en el diagrama de topología
Asignar el gateway predeterminado.	Asignar la primera dirección IP en la subred como gateway predeterminado.
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range
Asignar F0/18 a la VLAN 21	
Apagar todos los puertos sin usar	

Fuente: Autor.

## Switch S3

S3(config)#			
S3(config)#vlan 21 VLAN21	Se	configura	la
S3(config-vlan)#name Contabilidad nombre de la VLAN	Se	configura	el
S3(config-vlan)#exit			
S3(config)#vlan 23 VLAN23	Se	configura	la
S3(config-vlan)#name Ingenieria nombre de la VLAN	Se	configura	el
S3(config-vlan)#exit			
S3(config)#vlan 99 VLAN99	Se	configura	la
S3(config-vlan)#name Administracion nombre de la VLAN	Se	configura	el
S3(config-vlan)#exit			
S3(config)#interface vlan 99 de la VLAN 99	Se	habilita	la interfaz
S3(config-if)#ip add 192.168.99.3 255.255.255.0 direccionamiento de la interfaz	Se	configura	el
S3(config-if)#no shutdown interfaz	Se	enciende	la
S3(config-if)#exit			
S3(config)#ip default-gateway 192.168.99.1 dirección de la puerta de acceso por defecto	Se	configura	la
S3(config)#interface fa0/3 interfaz que es puerta troncal	Se	selecciona	la
S3(config-if)#switchport mode trunk modo troncal	Se	configuran	en
S3(config-if)#switchport trunk native vlan 1 como vlan nativa	Se	habilita	la VLAN 1
S3(config-if)#exit			
S3(config)#interface fa0/18			
S3(config-if)#switchport mode access interfaz con modo de acceso	Se	configura	la
S3(config-if)#switchport access vlan 23 23 para que circule en esta interfaz	Se	configura	la VLAN

S3(config-if)#exit  
 S3(config)# interface range fa0/1-2,fa0/4-17,fa0/19-24,gi0/1-2      Se seleccionan las interfaces que están inactivas  
 S3(config-if-range)#switchport mode access      Se configuran en modo de acceso  
 S3(config-if-range)#shutdown      Se desactivan las interfaces  
 S3(config-if-range)#exit

### Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 18. Tabla de configuración de subinterfaces en R1.

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	Descripción: LAN de Contabilidad Asignar la VLAN 21 Asignar la primera dirección disponible a esta interfaz
Configurar la subinterfaz 802.1Q .23 en G0/1	Descripción: LAN de Ingeniería Asignar la VLAN 23 Asignar la primera dirección disponible a esta interfaz
Configurar la subinterfaz 802.1Q .99 en G0/1	Descripción: LAN de Administración Asignar la VLAN 99 Asignar la primera dirección disponible a esta interfaz
Activar la interfaz G0/1	No shutdown

Fuente: Autor.

Router R1.

R1#configure terminal  
 R1(config)#interface gi0/1.21      Se configura la subinterfaz  
 R1(config-subif)#encapsulation dot1q 21      Se encapsula la subinterfaz y se le asigna la respectiva vlan  
 R1(config-subif)#description LAN de Contabilidad      Se configura una descripción de la subinterfaz

R1(config-subif)#ip add 192.168.21.1 255.255.255.0 direccionamiento de la subinterfaz R1(config-subif)#exit R1(config)#	Se configura el
R1(config)#interface gi0/1.23 subinterfaz	Se configura la
R1(config-subif)#encapsulation dot1q 23 subinterfaz y se le asigna la respectiva vlan	Se encapsula la
R1(config-subif)#description LAN de Ingenieria descripción de la subinterfaz	Se configura una
R1(config-subif)#ip add 192.168.23.1 255.255.255.0 direccionamiento de la subinterfaz R1(config-subif)#exit R1(config)#	Se configura el
R1(config)#interface gi0/1.99 subinterfaz	Se configura la
R1(config-subif)#encapsulation dot1q 99 subinterfaz y se le asigna la respectiva vlan	Se encapsula la
R1(config-subif)#description LAN de Administracion descripción de la subinterfaz	Se configura una
R1(config-subif)#ip add 192.168.99.1 255.255.255.0 direccionamiento de la subinterfaz R1(config-subif)#exit R1(config)#	Se configura el
R1(config)#interface gi0/1 interfaz	Se accede a la
R1(config-if)#no shutdown interfaz R1(config-if)#exit R1(config)#	Se enciende la

Paso 4: Verificar la conectividad de la red

Utilice el comando ping para probar la conectividad entre los switches y el R1.

Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 19. Tabla de verificaciones de la conectividad de la red.

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds: !!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
S3	R1, dirección VLAN 99	192.168.99.1	Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds: !!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/3 ms
S1	R1, dirección VLAN 21	192.168.21.1	Sending 5, 100-byte ICMP Echos to 192.168.21.1, timeout is 2 seconds: !!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
S3	R1, dirección VLAN 23	192.168.23.1	Sending 5, 100-byte ICMP Echos to 192.168.23.1, timeout is 2 seconds: !!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

Fuente: Autor.

Figura 15. Validación de ping desde S1 a R1, dirección VLAN 99.

```

S1
Physical Config CLI Attributes
IOS Command Line Interface

%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to
administratively down
S1(config-if-range)#exit
S1(config)#
%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed
state to up

S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#ping 192.168.99.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms

S1#ping 192.168.99.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

S1#
S1#

```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

ESP 1:55 a.m. 28/11/2021

Fuente: Autor.

Figura 16. Validación de ping desde S3 a R1, dirección VLAN 99.

```

S3
Physical Config CLI Attributes
IOS Command Line Interface

administratively down
%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to
administratively down
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to
administratively down
%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to
administratively down
S3(config-if-range)#exit
S3(config)#exit
S3#
%SYS-5-CONFIG_I: Configured from console by console

S3#ping 192.168.99.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms

S3#ping 192.168.99.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/3 ms

S3#

```

Ctrl+F6 to exit CLI focus

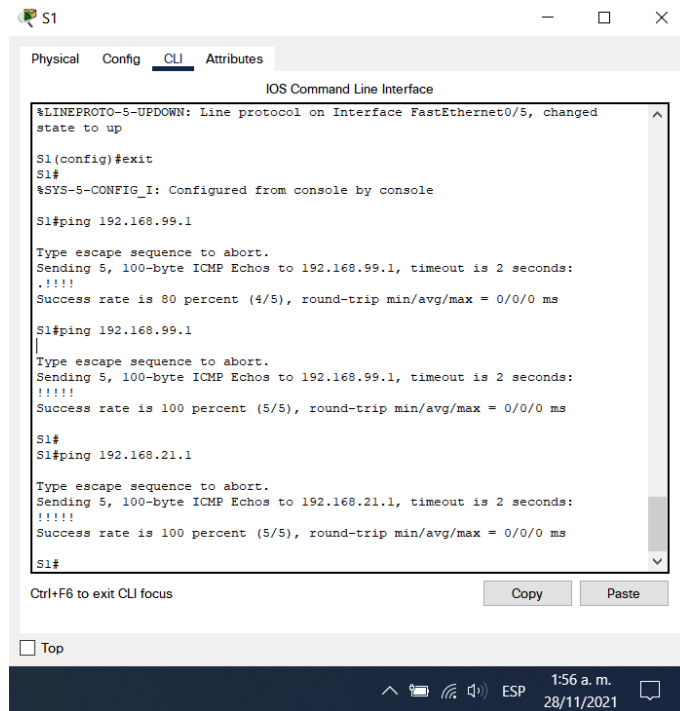
Copy Paste

Top

ESP 1:56 a.m. 28/11/2021

Fuente: Autor.

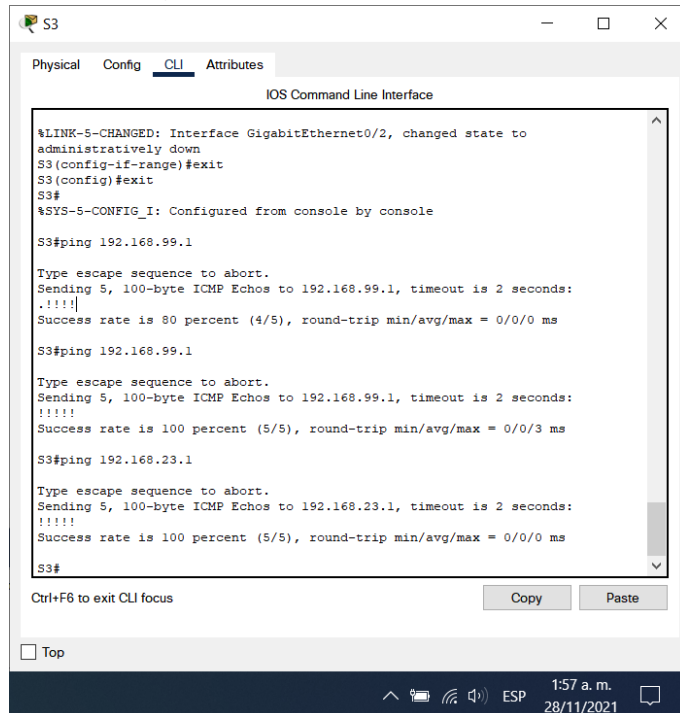
Figura 17. Validación de ping desde S1 a R1, dirección VLAN 21.



```
S1
Physical Config CLI Attributes
IOS Command Line Interface
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed
state to up
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console
S1#ping 192.168.99.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms
S1#ping 192.168.99.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
S1#
S1#ping 192.168.21.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.21.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
S1#
```

Fuente: Autor.

Figura 18. Validación de ping desde S3 a R1, dirección VLAN 23.



```
S3
Physical Config CLI Attributes
IOS Command Line Interface
%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to
administratively down
S3(config-if-range)#exit
S3(config)#exit
S3#
%SYS-5-CONFIG_I: Configured from console by console
S3#ping 192.168.99.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms
S3#ping 192.168.99.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/3 ms
S3#ping 192.168.23.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.23.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
S3#
```

Fuente: Autor.



#### Parte 4: Configurar el protocolo de routing dinámico OSPF

##### Paso 1: Configurar OSPF en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 20. Tareas de configuración para R1.

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	
Anunciar las redes conectadas directamente	Asigne todas las redes conectadas directamente.
Establecer todas las interfaces LAN como pasivas	
Desactive la sumarización automática	

Fuente: Autor.

##### Router R1.

R1(config)#router ospf 1 protocolo OSPF	Se habilita el
R1(config-router)#router-id 1.1.1.1 identificador de router	Se configura un
R1(config-router)#network 172.16.1.0 0.0.0.3 area 0	Se configura la
dirección general de la red conectada directamente, su wildcard y el área a asignar	
R1(config-router)#network 192.168.21.0 0.0.0.255 area 0	Se configura la
dirección general de la red conectada directamente, su wildcard y el área a asignar	
R1(config-router)#network 192.168.23.0 0.0.0.255 area 0	Se configura la
dirección general de la red conectada directamente, su wildcard y el área a asignar	
R1(config-router)#network 192.168.99.0 0.0.0.255 area 0	Se configura la
dirección general de la red conectada directamente, su wildcard y el área a asignar	
R1(config-router)#passive-interface gi0/1 interfaz como pasiva	Se configura la
R1(config-router)#passive-interface gi0/1.21 subinterfaz como pasiva	Se configura la
R1(config-router)#passive-interface gi0/1.23 subinterfaz como pasiva	Se configura la
R1(config-router)#passive-interface gi0/1.99 subinterfaz como pasiva	Se configura la

R1(config-router)#no auto-summary	Se desactiva la
sumarización automática	
R1(config-router)#exit	
R1(config)#interface gi0/1	
R1(config-if)#ip ospf 1 area 0	Se configura a la
interfaz	
R1(config-if)#exit	
R1(config)#interface se0/0/0	
R1(config-if)#ip ospf 1 area 0	Se configura a la
interfaz	
R1(config-if)#exit	

## Paso 2: Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 21. Tabla de configuración para R2.

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	
Anunciar las redes conectadas directamente	Nota: Omitir la red G0/0.
Establecer la interfaz LAN (loopback) como pasiva	
Desactive la sumarización automática.	

Fuente: Autor.

## Router R2.

R2(config)#router ospf 1	Se configura el
protocolo OSPF	
R2(config-router)#router-id 2.2.2.2	Se configura un
identificador de router	
R2(config-router)#network 10.10.10.10 0.0.0.0 area 0	Se configura la
dirección general de la red conectada directamente, su wildcard y el área a asignar	
R2(config-router)#network 172.16.1.0 0.0.0.3 area 0	Se configura la
dirección general de la red conectada directamente, su wildcard y el área a asignar	
R2(config-router)#network 172.16.2.0 0.0.0.3 area 0	Se configura la
dirección general de la red conectada directamente, su wildcard y el área a asignar	
R2(config-router)#passive-interface lo0	Se configura la
interfaz como pasiva	

R2(config-router)#no auto-summary	Se desactiva la
sumarización automática	
R2(config-router)#exit	
R2(config)#interface se0/0/0	
R2(config-if)#ip ospf 1 area 0	Se configura a la
interfaz	
R2(config-if)#exit	
R2(config)#interface se0/0/1	
R2(config-if)#ip ospf 1 area 0	Se configura a la
interfaz	
R2(config-if)#exit	

### Paso 3: Configurar OSPFv3 en el R3

La configuración del R3 incluye las siguientes tareas:

Tabla 22. Tareas de configuración para R2.

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	
Anunciar redes IPv4 conectadas directamente	
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	
Desactive la sumarización automática.	

Fuente: Autor.

### Router R3.

R3#configure terminal	
R3(config)#router ospf 1	Se configura el
protocolo OSPF	
R3(config-router)#router-id 3.3.3.3	Se configura un
identificador de router	
R3(config-router)#network 172.16.2.0 0.0.0.3 area 0	Se configura la
dirección general de la red conectada directamente, su wildcard y el área a asignar	
R3(config-router)#network 192.168.4.0 0.0.0.255 area 0	Se configura la
dirección general de la red conectada directamente, su wildcard y el área a asignar	
R3(config-router)#network 192.168.5.0 0.0.0.255 area 0	Se configura la
dirección general de la red conectada directamente, su wildcard y el área a asignar	

R3(config-router)#network 192.168.6.0 0.0.0.255 area 0	Se configura la
dirección general de la red conectada directamente, su wildcard y el área a asignar	
R3(config-router)#passive-interface lo4	Se configura la
interfaz como pasiva	
R3(config-router)#passive-interface lo5	Se configura la
interfaz como pasiva	
R3(config-router)#passive-interface lo6	Se configura la
interfaz como pasiva	
R3(config-router)#passive-interface lo7	Se configura la
interfaz como pasiva	
R3(config-router)#exit	
R3(config)#ipv6 unicast-routing	Se habilita el
direccionamiento unicast	
R3(config)#ipv6 router ospf 1	Se habilita OSPFv3
en el router	
R3(config-rtr)#router-id 3.3.3.3	Se configura un
identificador de ospf	
R3(config-rtr)#exit	
R3(config)#interface se0/0/1	
R3(config-if)#ipv6 ospf 1 area 0	Se configura la
interfaz	
R3(config-if)#exit	

#### Paso 4: Verificar la información de OSPF

Verifique que OSPF esté funcionando como se espera. Introduzca el comando de CLI adecuado para obtener la siguiente información:

Tabla 23. Verificación de la información de OSPF.

Pregunta	Respuesta
¿Con qué comando se muestran la ID del proceso OSPF, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?	Show ip protocols
¿Qué comando muestra solo las rutas OSPF?	Show ip route ospf
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	Show ip ospf interface

Fuente: Autor.

Figura 19. Verificación del ID del proceso OSPF, del router, las redes de routing y las interfaces pasivas en R1.

The screenshot shows the R1 CLI window with the following output:

```

R1#show ip pro
R1#show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 1.1.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.16.1.0 0.0.0.0.3 area 0
    192.168.21.0 0.0.0.255 area 0
    192.168.23.0 0.0.0.255 area 0
    192.168.99.0 0.0.0.255 area 0
  Passive Interface(s):
    GigabitEthernet0/1
    GigabitEthernet0/1.21
    GigabitEthernet0/1.23
    GigabitEthernet0/1.99
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1          110          00:03:29
    2.2.2.2          110          00:02:12
    3.3.3.3          110          00:01:55
    Distance: (default is 110)

R1#
R1#
  
```

Fuente: Autor

Figura 20. Verificación de las rutas OSPF en R1.

The screenshot shows the R1 CLI window with the following output:

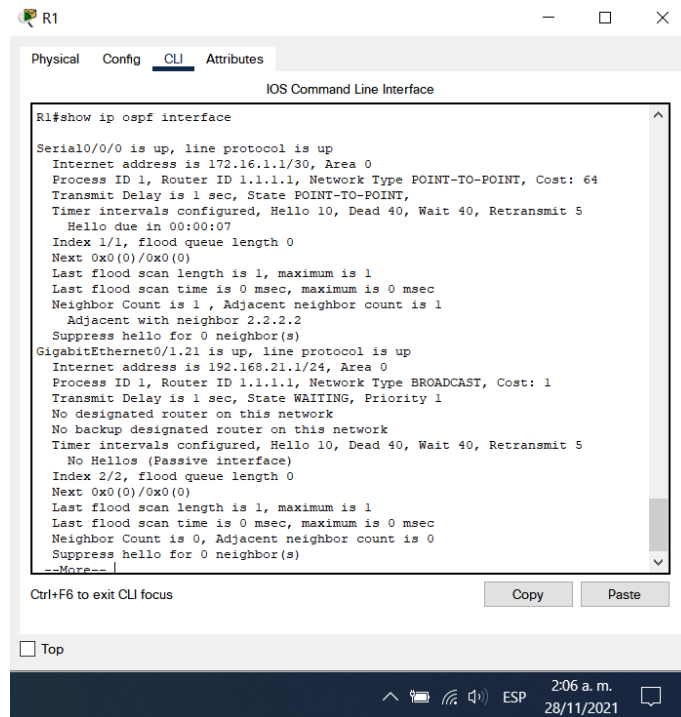
```

R1#show ip route ospf
O* 0.0.0.0 [110/1] via 0.0.0.0, 00:05:44, GigabitEthernet0/1
  10.0.0.0/32 is subnetted, 1 subnets
    10.10.10.10 [110/65] via 172.16.1.2, 00:04:04, Serial0/0/0
  172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
    172.16.2.0 [110/128] via 172.16.1.2, 00:04:04, Serial0/0/0
    192.168.4.0/32 is subnetted, 1 subnets
    192.168.4.1 [110/129] via 172.16.1.2, 00:02:30, Serial0/0/0
    192.168.5.0/32 is subnetted, 1 subnets
    192.168.5.1 [110/129] via 172.16.1.2, 00:02:30, Serial0/0/0
    192.168.6.0/32 is subnetted, 1 subnets
    192.168.6.1 [110/129] via 172.16.1.2, 00:02:30, Serial0/0/0

R1#
  
```

Fuente: Autor.

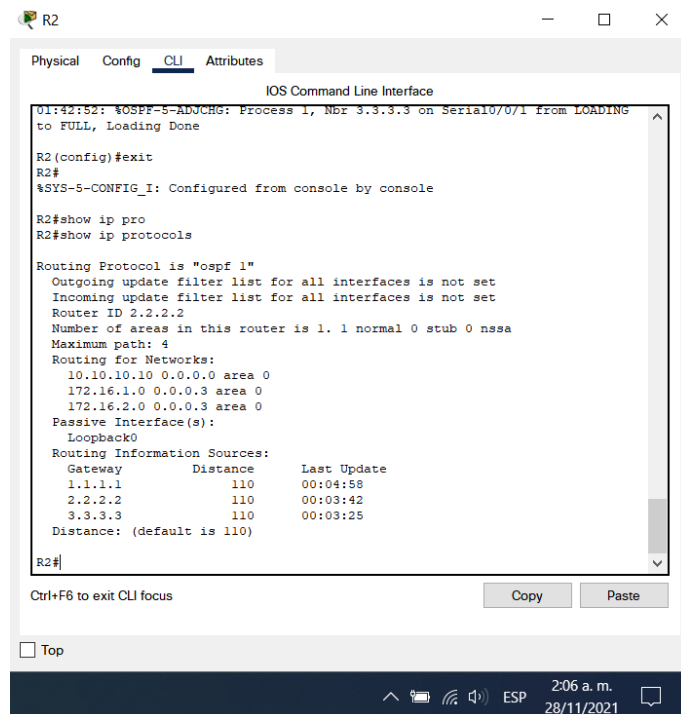
Figura 21. Verificación de sección de OSPF de la configuración en ejecución en R1.



```
R1#show ip ospf interface
Serial0/0/0 is up, line protocol is up
 Internet address is 172.16.1.1/30, Area 0
 Process ID 1, Router ID 1.1.1.1, Network Type POINT-TO-POINT, Cost: 64
 Transmit Delay is 1 sec, State POINT-TO-POINT,
 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
 Hello due in 00:00:07
 Index 1/1, flood queue length 0
 Next 0x0(0)/0x0(0)
 Last flood scan length is 1, maximum is 1
 Last flood scan time is 0 msec, maximum is 0 msec
 Neighbor Count is 1, Adjacent neighbor count is 1
   Adjacent with neighbor 2.2.2.2
 Suppress hello for 0 neighbor(s)
GigabitEthernet0/1.21 is up, line protocol is up
 Internet address is 192.168.21.1/24, Area 0
 Process ID 1, Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
 Transmit Delay is 1 sec, State WAITING, Priority 1
 No designated router on this network
 No backup designated router on this network
 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
 No Hellos (Passive interface)
 Index 2/2, flood queue length 0
 Next 0x0(0)/0x0(0)
 Last flood scan length is 1, maximum is 1
 Last flood scan time is 0 msec, maximum is 0 msec
 Neighbor Count is 0, Adjacent neighbor count is 0
 Suppress hello for 0 neighbor(s)
--More--
```

Fuente: Autor.

Figura 22. Verificación del ID del proceso OSPF, del router, las redes de routing y las interfaces pasivas en R2.



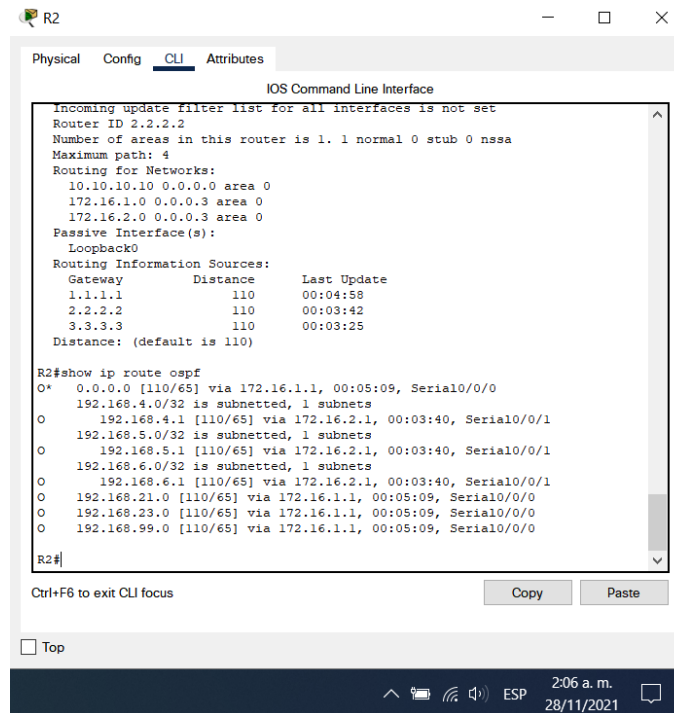
```
01:42:52: %OSPF-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/0/1 from LOADING
to FULL, Loading Done
R2(config)#exit
R2#
%SYS-5-CONFIG_I: Configured from console by console
R2#show ip pro
R2#show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 2.2.2.2
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    10.10.10.10 0.0.0.0 area 0
    172.16.1.0 0.0.0.3 area 0
    172.16.2.0 0.0.0.3 area 0
  Passive Interface(s):
    Loopback0
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1          110          00:04:58
    2.2.2.2          110          00:03:42
    3.3.3.3          110          00:03:25
  Distance: (default is 110)

R2#
```

Fuente: Autor

Figura 23. Verificación de las rutas OSPF en R2.



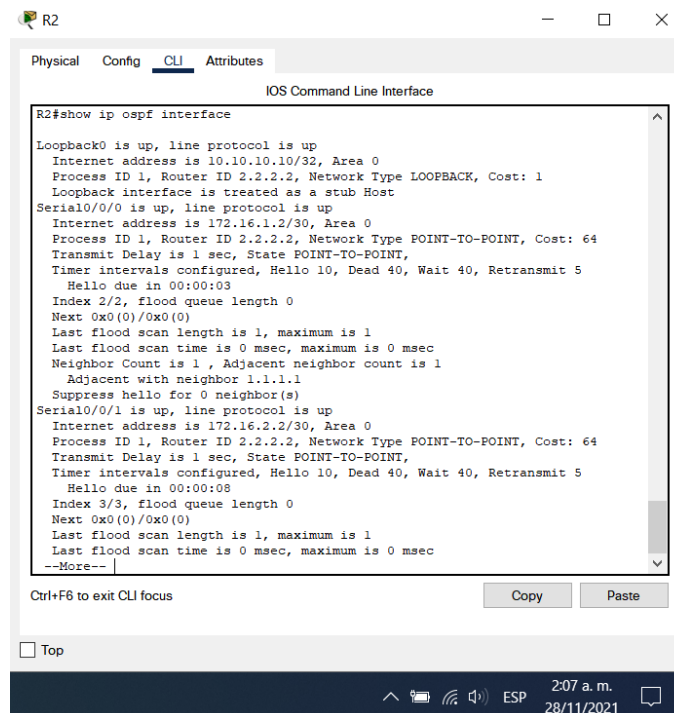
The screenshot shows the R2 CLI interface with the 'CLI' tab selected. The command 'show ip route ospf' has been executed, displaying the OSPF routing table. The output shows several routes, including the default route (0.0.0.0/0) and various subnets (192.168.4.0/32, 192.168.5.0/32, 192.168.6.0/32, 192.168.21.0/32, 192.168.23.0/32, 192.168.99.0/32) all learned via 172.16.1.1. The interface also shows the OSPF configuration, including the Router ID (2.2.2.2), the number of areas (1), and the maximum path count (4).

```
IOS Command Line Interface
Incoming update filter list for all interfaces is not set
Router ID 2.2.2.2
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Maximum path: 4
Routing for Networks:
  10.10.10.10 0.0.0.0 area 0
  172.16.1.0 0.0.0.3 area 0
  172.16.2.0 0.0.0.3 area 0
Passive Interface(s):
  Loopback0
Routing Information Sources:
  Gateway         Distance      Last Update
  1.1.1.1          110           00:04:58
  2.2.2.2          110           00:03:42
  3.3.3.3          110           00:03:25
Distance: (default is 110)

R2#show ip route ospf
O*  0.0.0.0 [110/65] via 172.16.1.1, 00:05:09, Serial0/0/0
O   192.168.4.0/32 is subnetted, 1 subnets
O     192.168.4.1 [110/65] via 172.16.2.1, 00:03:40, Serial0/0/1
O   192.168.5.0/32 is subnetted, 1 subnets
O     192.168.5.1 [110/65] via 172.16.2.1, 00:03:40, Serial0/0/1
O   192.168.6.0/32 is subnetted, 1 subnets
O     192.168.6.1 [110/65] via 172.16.2.1, 00:03:40, Serial0/0/1
O   192.168.21.0 [110/65] via 172.16.1.1, 00:05:09, Serial0/0/0
O   192.168.23.0 [110/65] via 172.16.1.1, 00:05:09, Serial0/0/0
O   192.168.99.0 [110/65] via 172.16.1.1, 00:05:09, Serial0/0/0
R2#
```

Fuente: Autor.

Figura 24. Verificación de sección de OSPF de la configuración en ejecución en R2.



The screenshot shows the R2 CLI interface with the 'CLI' tab selected. The command 'show ip ospf interface' has been executed, displaying the OSPF configuration for the interfaces. The output shows the configuration for Loopback0 and Serial0/0/0, including the interface status, IP address, area, process ID, router ID, network type, cost, and timer intervals.

```
IOS Command Line Interface
R2#show ip ospf interface
Loopback0 is up, line protocol is up
Internet address is 10.10.10.10/32, Area 0
Process ID 1, Router ID 2.2.2.2, Network Type LOOPBACK, Cost: 1
Loopback interface is treated as a stub Host
Serial0/0/0 is up, line protocol is up
Internet address is 172.16.1.2/30, Area 0
Process ID 1, Router ID 2.2.2.2, Network Type POINT-TO-POINT, Cost: 64
Transmit Delay is 1 sec, State POINT-TO-POINT,
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:03
Index 2/2, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1
Adjacent with neighbor 1.1.1.1
Suppress hello for 0 neighbor(s)
Serial0/0/1 is up, line protocol is up
Internet address is 172.16.2.2/30, Area 0
Process ID 1, Router ID 2.2.2.2, Network Type POINT-TO-POINT, Cost: 64
Transmit Delay is 1 sec, State POINT-TO-POINT,
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:08
Index 3/3, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
--More--
```

Fuente: Autor.

Figura 25. Verificación del ID del proceso OSPF, del router, las redes de routing y las interfaces pasivas en R3.

```

R3#
%SYS-5-CONFIG_I: Configured from console by console
R3#show ip pr
R3#show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 3.3.3.3
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.16.2.0 0.0.0.3 area 0
    192.168.4.0 0.0.0.255 area 0
    192.168.5.0 0.0.0.255 area 0
    192.168.6.0 0.0.0.255 area 0
  Passive Interface(s):
    Loopback4
    Loopback5
    Loopback6
    Loopback7
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1           110          00:05:55
    2.2.2.2           110          00:04:39
    3.3.3.3           110          00:04:22
  Distance: (default is 110)

R3#
  
```

Fuente: Autor

Figura 26. Verificación de las rutas OSPF en R3.

```

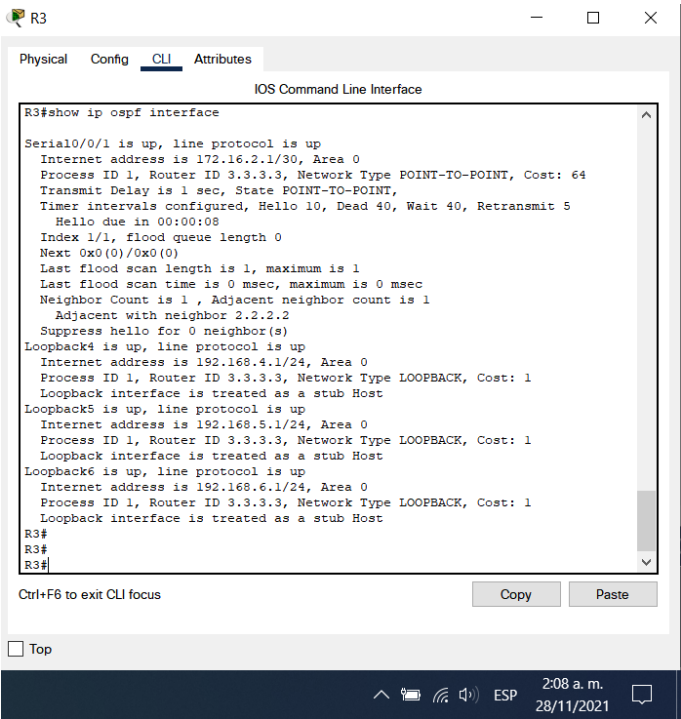
R3#show ip route ospf
O* 0.0.0.0 [110/129] via 172.16.2.2, 00:04:55, Serial0/0/1
  10.0.0.0/32 is subnetted, 1 subnets
O   10.10.10.10 [110/65] via 172.16.2.2, 00:04:55, Serial0/0/1
O   172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
O   172.16.1.0 [110/128] via 172.16.2.2, 00:04:55, Serial0/0/1
O   192.168.21.0 [110/129] via 172.16.2.2, 00:04:55, Serial0/0/1
O   192.168.23.0 [110/129] via 172.16.2.2, 00:04:55, Serial0/0/1
O   192.168.99.0 [110/129] via 172.16.2.2, 00:04:55, Serial0/0/1

R3#
  
```

Fuente: Autor.



Figura 27. Verificación de sección de OSPF de la configuración en ejecución en R3.



Fuente: Autor.

Parte 5: Implementar DHCP y NAT para IPv4

Paso 1: Configurar el R1 como servidor de DHCP para las VLAN 21 y 23

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 24. Tabla de configuración DHCP en R1 para las VLANS 21 y 23.

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	
Crear un pool de DHCP para la VLAN 21.	Nombre: ACCT Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado

Crear un pool de DHCP para la VLAN 23	Nombre: ENGR Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado
---------------------------------------	---

Fuente: Autor.

## Router R1

R1#configure terminal

R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20 Se excluyen las primeras 20 direcciones de la VLAN 21

R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20 Se excluyen las primeras 20 direcciones de la VLAN 23

R1(config)#ip dhcp pool ACCT Se configura un pool de DHCP para la VLAN 21

R1(dhcp-config)#network 192.168.21.0 255.255.255.0 Se configura la dirección de red

R1(dhcp-config)#default-router 192.168.21.1 Se configura la dirección de puerta de enlace

R1(dhcp-config)#dns-server 10.10.10.10 Se configura el servidor dns

R1(dhcp-config)#domain-name ccna-sa.com Se configura el nombre de dominio

R1(dhcp-config)#exit

R1(config)#ip dhcp pool ENGR Se configura un pool de DHCP para la VLAN 21

R1(dhcp-config)#network 192.168.23.0 255.255.255.0 Se configura la dirección de red

R1(dhcp-config)#default-router 192.168.23.1 Se configura la dirección de puerta de enlace

R1(dhcp-config)#dns-server 10.10.10.10 Se configura el servidor dns

R1(dhcp-config)#domain-name ccna-sa.com Se configura el nombre de dominio

R1(dhcp-config)#exit

R1(config)#

## Paso 2: Configurar la NAT estática y dinámica en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 25. Lista de tareas de configuración NAT estática y dinámica en R2.

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	Nombre de usuario: webuser Contraseña: cisco12345 Nivel de privilegio: 15
Habilitar el servicio del servidor HTTP	
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	
Crear una NAT estática al servidor web.	Dirección global interna: 209.165.200.237
Asignar la interfaz interna y externa para la NAT estática	
Configurar la NAT dinámica dentro de una ACL privada	Lista de acceso: 1 Permitir la traducción de las redes de Contabilidad y de Ingeniería en el R1 Permitir la traducción de un resumen de las redes LAN (loopback) en el R3
Defina el pool de direcciones IP públicas utilizables.	Nombre del conjunto: INTERNET El conjunto de direcciones incluye: 209.165.200.233 – 209.165.200.236
Definir la traducción de NAT dinámica	

Fuente: Autor.

### Router R2

```
R2#configure terminal
```

```
R2(config)#username webuser privilege 15 password cisco12345
```

 Se configura una cuenta de usuario con privilegios

```
R2(config)#ip nat inside source static 10.10.10.10 209.165.200.237
```

 Se configura la NAT que asigna la dirección de origen estático del servidor web

```
R2(config)#interface gi0/0
```

```
R2(config-if)#ip nat inside
```

 Se configura que la dirección NAT es dentro

```
R2(config-if)#exit
```

```
R2(config)#interface s0/0/0
```

R2(config-if)#ip nat outside	Se configura que la
dirección NAT es afuera	
R2(config-if)#exit	
R2(config)#interface s0/0/1	
R2(config-if)#ip nat inside	Se configura que la
dirección NAT es dentro	
R2(config-if)#exit	
R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255	Se configura una lista
de acceso que permita la VLAN 21	
R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255	Se configura una lista
de acceso que permita la VLAN 23	
R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255	Se cr configura ea una
lista de acceso que permita la dirección resumida de las loopback de R3	
R2(config)#ip nat pool INTERNET 209.165.200.233 209.165.200.236 netmask	Se configura el pool
255.255.255.248	
NAT de direcciones públicas que son utilizables	
R2(config)#ip nat inside source list 1 pool INTERNET	Se configura la
traducción de NAT dinámicamente	
R2(config)#	

### Paso 3: Verificar el protocolo DHCP y la NAT estática

Utilice las siguientes tareas para verificar que las configuraciones de DHCP y NAT estática funcionen de forma correcta. Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

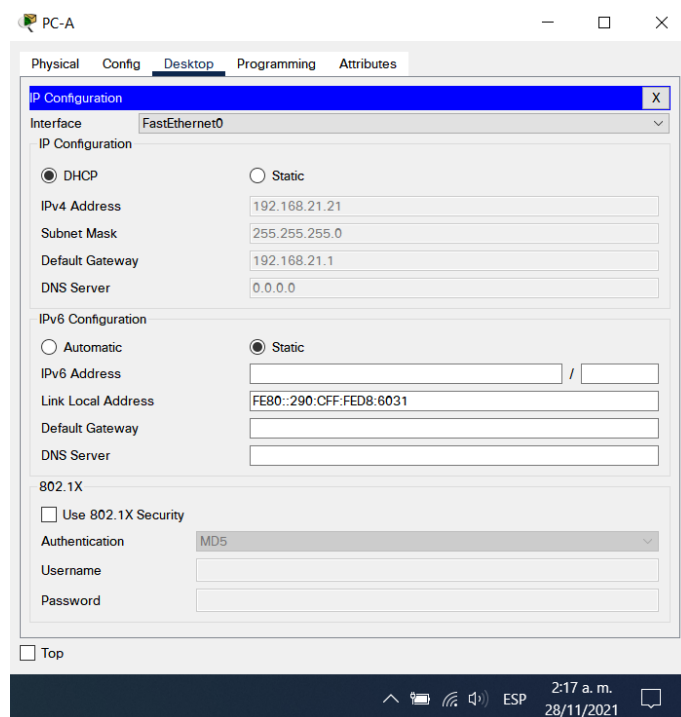
Tabla 26. Tabla de verificación del protocolo DHCP y la NAT estática.

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Si
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Si

<p>Verificar que la PC-A pueda hacer ping a la PC-C</p> <p>Nota: Quizá sea necesario deshabilitar el firewall de la PC.</p>	<p>Ping statistics for 192.168.23.21: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milliseconds: Minimum = 0ms, Maximum = 1ms, Average = 0ms</p>
<p>Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.229)</p> <p>Iniciar sesión con el nombre de usuario webuser y la contraseña cisco12345</p>	<p>No funciona porque packet tracer no soporta configurar un router como servidor web</p>

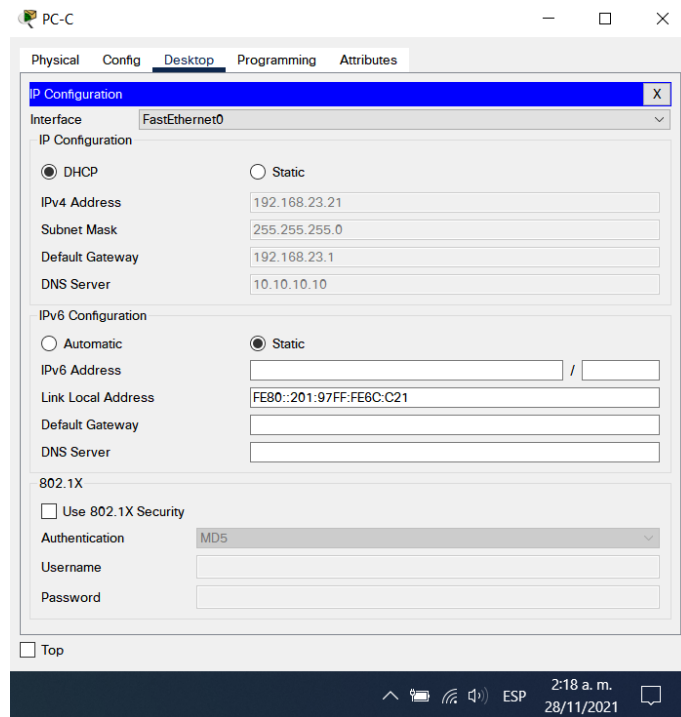
Fuente: Autor.

Figura 28. Verificación del direccionamiento DHCP en PC-A.



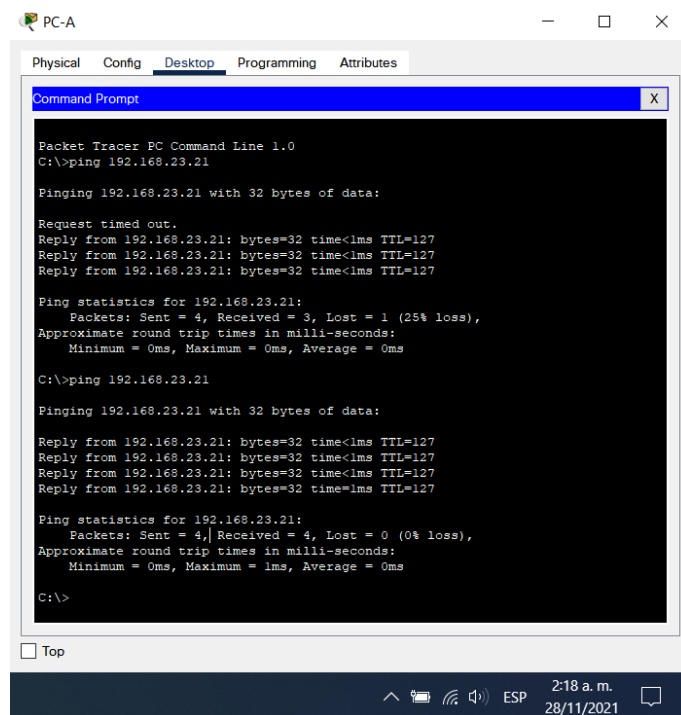
Fuente: Autor.

Figura 29. Verificación del direccionamiento DHCP en PC-C.



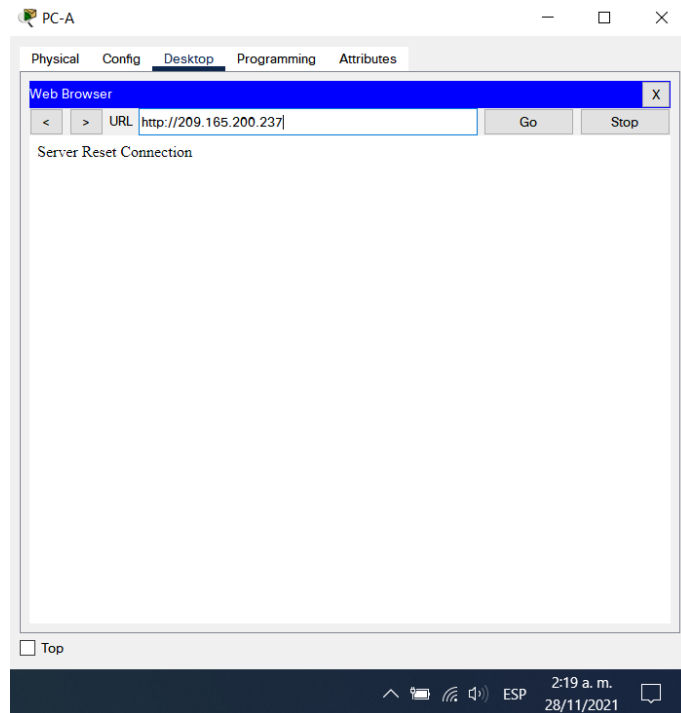
Fuente: Autor.

Figura 30. Verificación del ping entre PC-A y PC-C.



Fuente: Autor.

Figura 31. Verificación de la conexión al servidor web desde el PC-A.



Fuente: Autor.

## Parte 6: Configurar NTP

Tabla 27. Lista de tareas de configuración NTP.

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	5 de marzo de 2016, 9 a. m.
Configure R2 como un maestro NTP.	Nivel de estrato: 5
Configurar R1 como un cliente NTP.	Servidor: R2
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	Ntp update-calendar
Verifique la configuración de NTP en R1.	Show ntp associations

### Router R2

R2# clock set 2:20:10 28 November 2021  
en el router

Se configura la hora

R2(config)#ntp master 5  
como maestro NTP

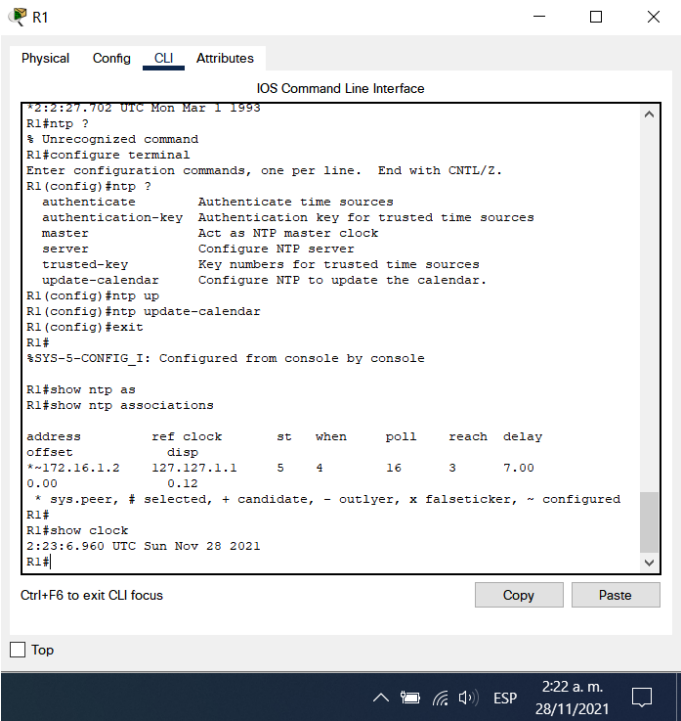
Se configura el router

Router R1

R1#configure terminal  
R1(config)#ntp server 172.16.1.2  
como cliente NTP  
R1(config)#ntp update-calendar  
que actualice el calendario periodicamente

Se configura el router  
  
Se configura para

Figura 32. Verificación de la configuración NTP en R1.



Fuente: Autor.

Parte 7: Configurar y verificar las listas de control de acceso (ACL)

Paso 1: Restringir el acceso a las líneas VTY en el R2

Tabla 28. Lista de tareas de configuración y verificación de listas de control de acceso en R2.

Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	Nombre de la ACL: ADMIN-MGT



Aplicar la ACL con nombre a las líneas VTY	
Permitir acceso por Telnet a las líneas de VTY	
Verificar que la ACL funcione como se espera	

Fuente: Autor.

Router R2.

R2#configure terminal

R2(config)#ip access-list standard ADMIN-MGT  
de acceso estándar nombrada

Se configura una lista

R2(config-std-nacl)#permit host 172.16.1.1  
permita la dirección ip del router R1

Se especifica que solo

R2(config-std-nacl)#exit

R2(config)#line vty 0 4

R2(config-line)#access-class ADMIN-MGT in  
de acceso en la línea de telnet

Se configura la lista

R2(config-line)#transport input telnet  
transporte de entrada sea telnet

Se habilita que el

R2(config-line)#exit

R2(config)#

Figura 33. Verificación de la ACL en PC-A.

```

PC-A
Physical Config Desktop Programming Attributes
Command Prompt

Pinging 192.168.23.21 with 32 bytes of data:
Request timed out.
Reply from 192.168.23.21: bytes=32 time<1ms TTL=127
Reply from 192.168.23.21: bytes=32 time<1ms TTL=127
Reply from 192.168.23.21: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.23.21:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.23.21

Pinging 192.168.23.21 with 32 bytes of data:

Reply from 192.168.23.21: bytes=32 time<1ms TTL=127
Reply from 192.168.23.21: bytes=32 time<1ms TTL=127
Reply from 192.168.23.21: bytes=32 time<1ms TTL=127
Reply from 192.168.23.21: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.23.21:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
C:\>telnet 172.16.1.2
Trying 172.16.1.2 ...
% Connection refused by remote host
C:\>|
  
```

Fuente: Autor.

Figura 34. Verificación de la ACL en R1.

```

R1
Physical Config CLI Attributes
IOS Command Line Interface

trusted-key Key numbers for trusted time sources
update-calendar Configure NTP to update the calendar.
R1(config)#ntp up
R1(config)#ntp update-calendar
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#show ntp as
R1#show ntp associations

address      ref clock      st  when  poll  reach  delay
offset      disp
*~172.16.1.2  127.127.1.1    5   4      16    3      7.00
0.00        0.12
* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
R1#
R1#show clock
2:23:6.960 UTC Sun Nov 28 2021
R1#
R1#telnet 172.16.1.2
Trying 172.16.1.2 ...OpenEl acceso sin permiso queda prohibido

User Access Verification

Password:
R2>enable
Password:
R2#|
  
```

Fuente: Autor.

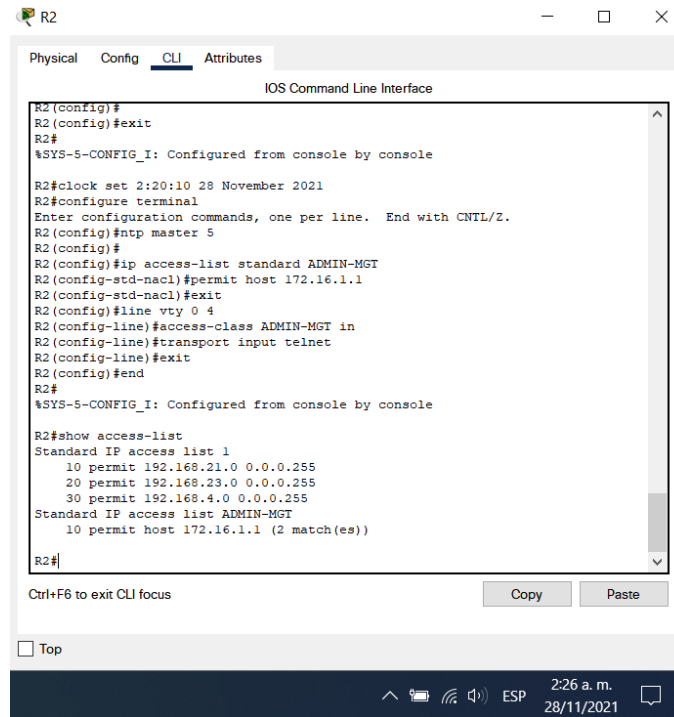
Paso 2: Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente

Tabla 29. Lista de tareas de verificación de comando CLI.

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	R2#show access-list
Restablecer los contadores de una lista de acceso	R2#clear ip access-list counters
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	R2#show ip interface
¿Con qué comando se muestran las traducciones NAT?	Nota: Las traducciones para la PC-A y la PC-C se agregaron a la tabla cuando la computadora de Internet intentó hacer ping a esos equipos en el paso 2. Si hace ping a la computadora de Internet desde la PC-A o la PC-C, no se agregarán las traducciones a la tabla debido al modo de simulación de Internet en la red.
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	Clear ip nat translation *

Fuente: Autor.

Figura 35. Mostrar las coincidencias recibidas luego de ser establecida en R2.



```
R2
Physical Config CLI Attributes
IOS Command Line Interface
R2(config)#
R2(config)#exit
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#clock set 2:20:10 28 November 2021
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ntp master 5
R2(config)#
R2(config)#ip access-list standard ADMIN-MGT
R2(config-std-nacl)#permit host 172.16.1.1
R2(config-std-nacl)#exit
R2(config)#line vty 0 4
R2(config-line)#access-class ADMIN-MGT in
R2(config-line)#transport input telnet
R2(config-line)#exit
R2(config)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#show access-list
Standard IP access list 1
  10 permit 192.168.21.0 0.0.0.255
  20 permit 192.168.23.0 0.0.0.255
  30 permit 192.168.4.0 0.0.0.255
Standard IP access list ADMIN-MGT
  10 permit host 172.16.1.1 (2 match(es))

R2#
```

Ctrl+F6 to exit CLI focus

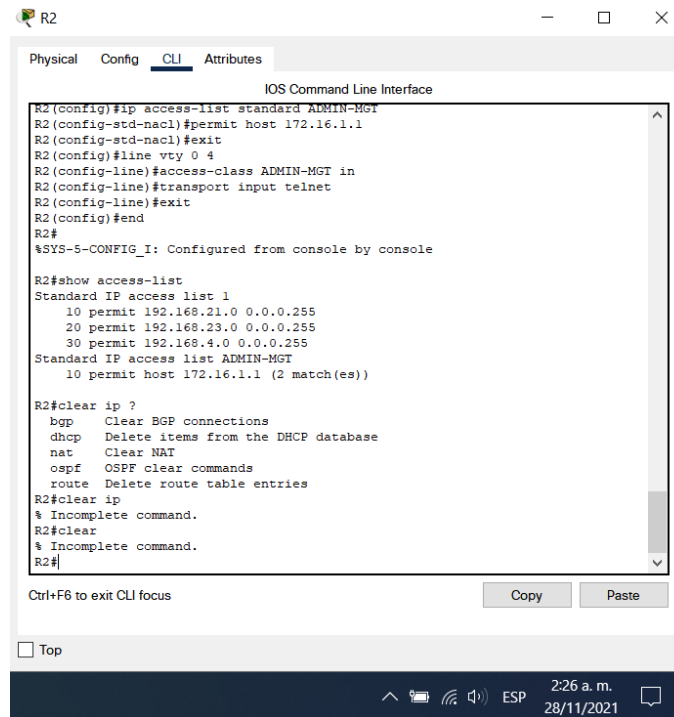
Copy Paste

Top

2:26 a.m. 28/11/2021

Fuente: Autor.

Figura 36. Restablecer los contadores de una lista de acceso.



```
R2
Physical Config CLI Attributes
IOS Command Line Interface
R2(config)#ip access-list standard ADMIN-MGT
R2(config-std-nacl)#permit host 172.16.1.1
R2(config-std-nacl)#exit
R2(config)#line vty 0 4
R2(config-line)#access-class ADMIN-MGT in
R2(config-line)#transport input telnet
R2(config-line)#exit
R2(config)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#show access-list
Standard IP access list 1
  10 permit 192.168.21.0 0.0.0.255
  20 permit 192.168.23.0 0.0.0.255
  30 permit 192.168.4.0 0.0.0.255
Standard IP access list ADMIN-MGT
  10 permit host 172.16.1.1 (2 match(es))

R2#clear ip ?
    bgp      Clear BGP connections
    dhcp      Delete items from the DHCP database
    nat       Clear NAT
    ospf      OSPF clear commands
    route     Delete route table entries
R2#clear ip
% Incomplete command.
R2#clear
% Incomplete command.
R2#
```

Ctrl+F6 to exit CLI focus

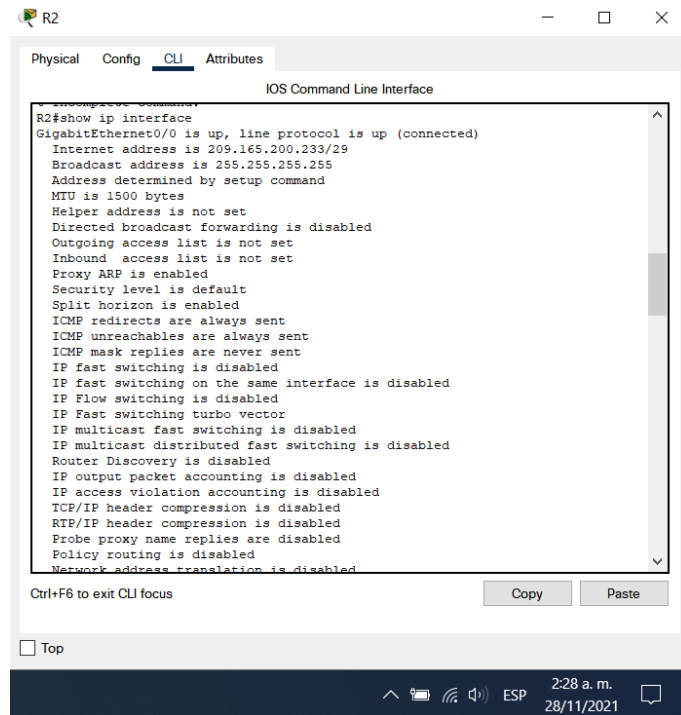
Copy Paste

Top

2:26 a.m. 28/11/2021

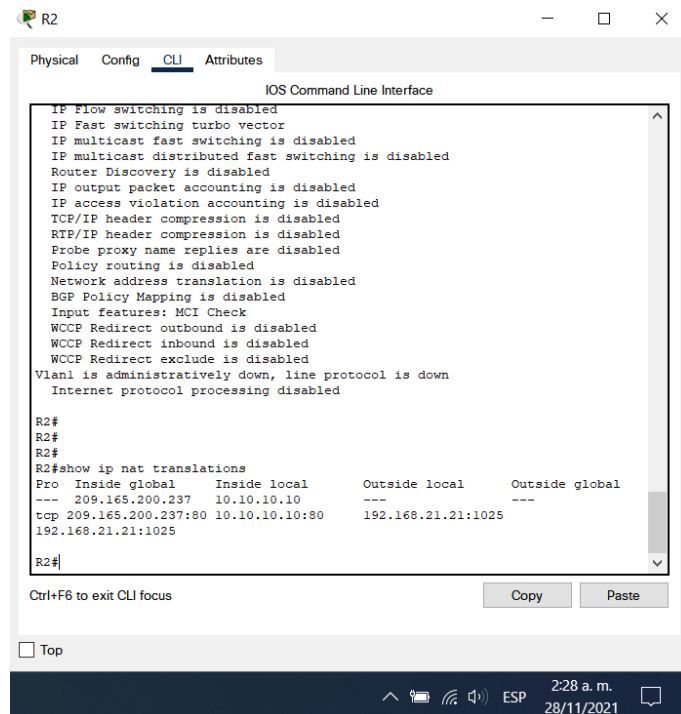
Fuente: Autor.

Figura 37. Mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica.



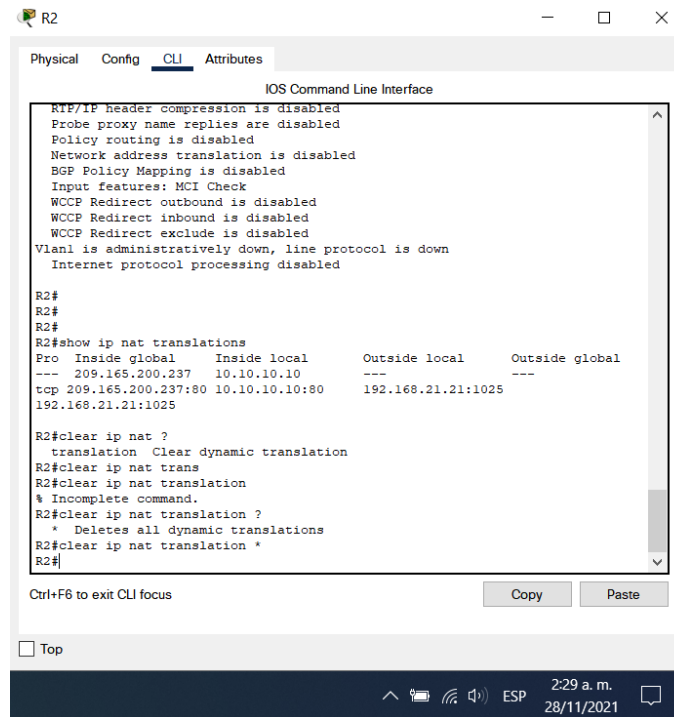
Fuente: Autor.

Figura 38. Mostrar las traducciones NAT.



Fuente: Autor.

Figura 39. Comando utilizado para eliminar las traducciones de NAT dinámicas.



The screenshot shows a Cisco IOS Command Line Interface window titled "R2" with tabs for "Physical", "Config", "CLI", and "Attributes". The "CLI" tab is active, displaying the following text:

```
RTF/IP header compression is disabled
Probe proxy name replies are disabled
Policy routing is disabled
Network address translation is disabled
BGP Policy Mapping is disabled
Input features: MCI Check
WCCP Redirect outbound is disabled
WCCP Redirect inbound is disabled
WCCP Redirect exclude is disabled
Vlan1 is administratively down, line protocol is down
Internet protocol processing disabled

R2#
R2#
R2#
R2#show ip nat translations
Pro  Inside global  Inside local  Outside local  Outside global
---  209.165.200.237  10.10.10.10   ---           ---
tcp  209.165.200.237:80 10.10.10.10:80 192.168.21.21:1025
192.168.21.21:1025

R2#clear ip nat ?
translation  Clear dynamic translation
R2#clear ip nat trans
R2#clear ip nat translation
% Incomplete command.
R2#clear ip nat translation ?
* Deletes all dynamic translations
R2#clear ip nat translation *
R2#
```

Below the terminal window, there are buttons for "Copy" and "Paste", and a "Top" button. The system tray at the bottom shows the time as 2:29 a.m. on 28/11/2021.

Fuente: Autor.

## CONCLUSIONES

Con el desarrollo de esta prueba de habilidades se pone en practica los conceptos adquiridos en el transcurso del diplomado de profundización y permite adquirir destrezas que permitan solucionar problemas relacionados con la configuración de redes pequeñas como la propuesta en el escenario 1, que comprende la construcción de la simulación de la red con la herramienta packet tracer, el desarrollo de esquemas de direccionamiento ip en el que se detallan las estructuras de los dispositivos, sus características y que sean admisibles a la implementación de direcciones IPv4 e IPv6. Además, la forma de como se obtenienen sus distintas subredes a partir del calculo de la dirección general y su respectiva máscara de red.

Por otra parte, se aplican conceptos que están relacionados con la aplicación de seguridad, que va desde la aplicación de SSH en vez de TELNET; la aplicación de servicios de cifrados de clave de texto plano, la asignación de claves a la línea de consola y la línea de terminal, la asignación de banners que informen al administrador, advertencias sobre el uso inadecuado o accesos no autorizados a los dispositivos, la configuración de direccionamiento en cada una de las interfaces, tanto físicas como lógicas y la verificación de la conectividad entre los host y los dispositivos.

Finalmente, estos desafíos se manifiestan a través de escenarios de diferentes estructuras, diseños y soluciones de red. En el segundo escenario se implementa el protocolo de enrutamiento OSPF para conectar diferentes sub- La aplicación del concepto entre red y VLAN en uno de ellos, la adecuación de servicios DHCP que permita facilitar la obtención de direcciones ip por parte de sus equipos host de diferente VLAN, la configuración del protocolo de internete que permita sincronizar los relojes de dos routers diferentes y la implementación de la traducción de direcciones de red NAT.

## BIBLIOGRAFÍA

CISCO. (2019). Acceso a la red. Fundamentos de Networking. Recuperado de: <https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#4>

CISCO. (2019). Capa de aplicación. Fundamentos de Networking. Recuperado de: <https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#10>

CISCO. (2019). Capa de red. Fundamentos de Networking. Recuperado de: <https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#6>

CISCO. (2019). Capa de transporte. Fundamentos de Networking. Recuperado de: <https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#9>

CISCO. (2019). Conceptos de Routing. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#1>

CISCO. (2019). Configuración de un sistema operativo de red. Fundamentos de Networking. Recuperado de: <https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#2>

CISCO. (2019). Configuración de un sistema operativo de red. Fundamentos de Networking. Recuperado de: <https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#11>

CISCO. (2019). Configuración del Switch. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#5>

CISCO. (2019). Detección, Administración y Mantenimiento de Dispositivos. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#10>

CISCO. (2019). DHCP. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#8>

CISCO. (2019). Direccionamiento IP. Fundamentos de Networking. Recuperado de: <https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#7>



CISCO. (2019). División de redes IP en subredes. Fundamentos de Networking. Recuperado de: <https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#8>

CISCO. (2019). Ethernet. Fundamentos de Networking. Recuperado de: <https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#5>

CISCO. (2019). Exploración de la red. Fundamentos de Networking. Recuperado de: <https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#1>

CISCO. (2019). Listas de Control de Acceso. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#7>

CISCO. (2019). NAT para IPv4. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#9>

CISCO. (2019). Protocolos y comunicaciones de red. Fundamentos de Networking. Recuperado de: <https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#3>

CISCO. (2019). Redes Conmutadas. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#4>

CISCO. (2019). Routing Dinámico. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#3>

CISCO. (2019). Routing Estático. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#2>

CISCO. (2019). VLAN. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#6>

UNAD (2017). Configuración de Switches y Routers [OVA]. Recuperado de <https://1drv.ms/u/s!AmlJYei-NT1lhqL9QChD1m9EuGqC>

UNAD (2017). Principios de Enrutamiento [OVA]. Recuperado de [https://1drv.ms/u/s!AmIJYei-NT1lhgOyjWeh6timi\\_Tm](https://1drv.ms/u/s!AmIJYei-NT1lhgOyjWeh6timi_Tm)

Vesga, J. (2014). Diseño y configuración de redes con Packet Tracer [OVA]. Recuperado de [https://1drv.ms/u/s!AmIJYei-NT1lhgCT9VCtl\\_pLtPD9](https://1drv.ms/u/s!AmIJYei-NT1lhgCT9VCtl_pLtPD9)

Vesga, J. (2017). Ping y Tracer como estrategia en los procesos de Networking [OVA]. Recuperado de <https://1drv.ms/u/s!AmIJYei-NT1lhgTCtKY-7F5KIRC3>